IFSH
IFAR

WORKING PAPER #6
Juli 2005

TERRORGEFAHR UND DIE VERWUNDBARKEIT MODERNER INDUSTRIESTAATEN: WIE GUT IST DEUTSCHLAND VORBEREITET?

Jan Kuhn / Götz Neuneck

Forschungsstudie im Auftrag der

anderes lernen e.V.

Heinrich Böll Stiftung Schleswig Holstein

Interdisziplinäre Forschungsgruppe Abrüstung und Rüstungskontrolle

Institute for Peace Research and Security Policy at the University of Hamburg
Falkenstein 1, 22587 Hamburg
Tel: +49 40 866 077-0 - Fax: +49 40 866 36 15

GRUPPENPROFIL

Die „Interdisziplinäre Forschungsgruppe Abrüstung und Rüstungskontrolle (IFAR)“ beschäftigt sich mit dem komplexen Zusammenspiel von rüstungsdynamischen Faktoren, dem potenziellen Waffeneinsatz, der Strategiedebatte sowie den Möglichkeiten von Rüstungskontrolle und Abrüstung als sicherheitspolitische Instrumente. Der Schwerpunkt der Arbeit liegt dabei auf folgenden Forschungslinien:

- Grundlagen, Möglichkeiten und Formen von Rüstungskontrolle, Abrüstung und Nonproliferation nach dem Ende des Ost-West-Konfliktes sowie die Entwicklung von anwendungsbezogenen Konzepten präventiver Rüstungskontrolle

- „Monitoring“ der fortschreitenden Rüstungsdynamik und Rüstungskontrollpolitik in Europa und weltweit mit Fokus auf moderne Technologien

- Technische Möglichkeiten existierender und zukünftiger (Waffen-) Entwicklungen, besonders im Bereich Raketenabwehr und Weltraumbewaffnung

Der steigenden Komplexität solcher Fragestellungen wird in Form einer interdisziplinär arbeitenden Forschungsgruppe Rechnung getragen. Die Arbeitsweise zeichnet sich durch die Kombination von natur- und sozialwissenschaftlichen Methoden und Expertisen aus. Durch die intensiven Kooperationen mit anderen Institutionen unterschiedlicher Disziplinen wird insbesondere Grundlagenforschung im Bereich der naturwissenschaftlich-technischen Dimension von Rüstungskontrolle geleistet. Darüber hinaus beteiligt sich IFAR auch an einer Reihe von Expertennetzwerken, die Expertisen aus Forschung und Praxis zusammenführen und Forschungsanstrengungen bündeln.

Die Arbeitsgruppe hat eine langjährige Expertise in den Bereichen kooperative Rüstungssteuerung und Rüstungstechnologien sowie verschiedene wissenschaftlichen Kernkompetenzen aufgebaut. Diese flossen in die international vielbeachteten Beiträge des IFSH zur Rüstungskontrolle ein, so das Konzept der 'kooperativen Rüstungssteuerung' sowie Studien zur konventionellen und nuklearen Rüstung und Abrüstung, zur Bewertung technologischer Rüstungsprozesse, zur strategischen Stabilität, zur strukturellen Angriffsunfähigkeit sowie zur Vertrauensbildung und europäischen Sicherheit.

IFAR bietet verschiedene Formen der Nachwuchsförderung an. Neben Lehrtätigkeiten gemeinsam mit der Universität Hamburg und im Studiengang 'Master of Peace and Security Studies' können auch Praktika in der Arbeitsgruppe absolviert werden.

Die Arbeitsgruppe kooperiert mit einer Vielzahl von nationalen und internationalen Organisationen.

Kontakt:
Götz Neuneck
Interdisziplinäre Forschungsgruppe Abrüstung und Rüstungskontrolle IFAR

Institute for Peace Research and Security Policy at the University of Hamburg
Falkenstein 1, 22587 Hamburg
Tel: +49 40 866 077-0 Fax: +49 40 866 36 15
ifar@ifsh.de www.ifsh.de
Webpage zur Rüstungskontrolle: www.armscontrol.de

TERRORGEFAHR UND DIE VERWUNDBARKEIT MODERNER INDUSTRIESTAATEN: WIE GUT IST DEUTSCHLAND VORBEREITET?

> Die Terroranschläge von Madrid unterstreichen eine neue und in dieser Art in Europa noch nicht erlebte Verletzlichkeit der Gesellschaften. (Peter Struck 2004)
>
> Die Anschläge haben uns die Illusion genommen, die wirtschaftlichen, politischen, kulturellen Abhängigkeiten seien einseitig, die erfolgreichen westlichen Gesellschaften unverwundbar. (Wolfgang Thierse 2001)
>
> Unsere modernen Industriegesellschaften sind verletzlich. Das gilt insbesondere gegenüber einem „gesichtslosen Gegner", der skrupellos genug ist, überall und zu jeder Zeit zuzuschlagen und dabei das eigene Leben nicht zu achten. (Bernhard Vogel 2002)
>
> Die Terroranschläge vom 11. September 2001 haben die Wahrnehmung der Welt verändert. Sie haben gezeigt, dass der internationale Terrorismus eine der größten Gefahren für den Weltfrieden ist, und verdeutlicht, wie verletzlich unsere offenen, demokratischen Gesellschaften sind. (Auswärtiges Amt 2002)
>
> Die schrecklichen Angriffe auf das World Trade Center in den USA haben uns vor Augen geführt, wie verletzlich unsere moderne, offene, freiheitliche Gesellschaft ist. (Angela Merkel 2001)

Einleitung[1]

Westliche Industrienationen, wie die Staaten der EU, USA, Kanada, Japan oder Australien sind strukturell verwundbar. Diese Erkenntnis besteht nicht erst seit den Anschlägen vom 11. September 2001 in den USA oder denen vom 11. März 2004 in Madrid. Vielmehr ist die Erkenntnis über Gefahren, die durch Angriffe auf Elemente der Industrie- und Produktionsstrukturen westlicher Staaten ausgehen, schon in den 1980er Jahren diskutiert worden.[2] Insbesondere wurde argumentiert, dass auch ein konventionell geführter Krieg die industrialisierten Gesellschaften zerstören würde, die das Militär eigentlich schützen sollte. So wurden die Angriffe mit konventioneller Munition auf Atomkraftwerke, Raffinerien oder wichtige Industriezentren durchdacht. Damals wurde, im Gegensatz zu heute, von einem militärischen Konflikt zwischen Staaten ausgegangen. Die Lösung des Problems, zumindest die der Friedensforschung, bestand u.a. in der Empfehlung, das Militär kurzfristig so umzubauen, dass es nur noch defensive Aufgaben wahrnehmen könne bzw. mittels Rüstungskontrollvereinbarungen abzurüsten.[3] Langfristig sollte es dann zu einer vollständigen Abrüstung kommen, da, nach Meinung einiger Autoren, Militär und moderne Zivilisationen nicht kompatibel seien.[4] Heute stellt sich das Problem in Bezug auf die Verwundbarkeit ähnlich, die politische Situation aber anders da. Wurde während des Kalten Kriegs über militärische Auseinandersetzungen zwischen Staaten nachgedacht, werden heute Anschläge

[1] Die Autoren danken Pia Kohorst, André Rothkirch und Achim Maas für wertvolle Hinweise und Anmerkungen.

[2] Siehe hierzu Gonnermann, Bernhard / Mechtersheimer, Alfred (1990) (Hrsg.): *Verwundbarer Frieden Zwang zur gemeinsamen Sicherheit für die Industriegesellschaften Europas*, Brandenburgisches Verlagshaus.

[3] Dieses sollte erfolgen, indem beispielsweise Panzerverbände abgebaut würden und generell auf raumgebundene Einheiten im Gegensatz zu flexiblen Einheiten zurückgegriffen würde. Raumgebundene Einheiten wären lediglich zu Defensivaktionen fähig gewesen.

[4] Vogt, Wolfgang R. (1990): *Militär als Altlast – ein Fall friedenspolitischer Entsorgung?*, in Gonnermann / Mechtersheim (1990), S. 133-152, S. 146f.

durch „substaatliche Akteure“ befürchtet.[5] Der neue „Gegner“ erfordert neue und andere Strategien als der alte, da nur in einem sehr engen Maße auf Abschreckung oder Kooperation gesetzt werden kann, die „Rationalität“ der Akteure unterschiedlich und die Effizienz von terroristischen Angriffen auf Infrastrukturen schwer nachweisbar ist.

Der Umgang mit der Verletzlichkeit eines entwickelten Industriestaates wie Deutschland Umfasst ein breites Spektrum und kann zwischen zwei verschiedenen Extrempunkten liegen. Die Position im einen Extrem fragt nicht nach den Bedrohungen, sondern nach den eigenen Verwundbarkeiten. Das Ziel ist dann der Versuch, alle erdenklichen Schwachstellen der Gesellschaft schließen zu wollen, um sich immun gegen Angriffe auf die Infrastrukturen des Staates zu machen. Im Zuge dessen ist zu erwarten, dass die Waage zwischen Sicherheit und Freiheit mehr in Richtung Sicherheit und einer starken Einschränkung von Bürgerrechten ausschlagen wird. Das andere Extrem analysiert nicht die eigenen Fähigkeiten, sondern die Bedrohung. Dies hat den Vorteil, dass man nicht gezwungen ist, alles „sicherer“ zu machen, sondern sich auf bestimmte Orte oder Strukturen beschränken kann. Es hat aber den Nachteil, dass die Bedrohung falsch eingeschätzt werden könnte und es dadurch zu „unvorstellbaren“ Ereignissen kommen kann, die wiederum die Bedrohungsängste schüren und neue verschärfte Sicherheitsstrategien implizieren.

Betrachtet man die erste Sichtweise und achtet nur auf die Verwundbarkeit und die eigenen Fähigkeiten, sollte man sich darüber Gedanken machen, welche Schutzmaßnahmen erfolgreich sein könnten. Hierbei stellt sich die Frage, ob Schutz unter der Verschärfung von Gesetzen und Einschränkungen von Bürgerrechten wesentlich effizienter und besser gestaltet werden kann. Lautet die Antwort ja, so folgt die Frage, wie viele Rechte aufgegeben werden müßten, um eine bestimmte Schutzstufe zu erlangen. Es verbleibt jedoch die Frage, ob ein umfassender Schutz wirklich erforderlich ist und jemals erfolgreich sein kann.

Die Begriffe Bedrohung und Verwundbarkeit bilden dabei zentrale Elemente in der öffentlichen wie wissenschaftlichen Debatte. Gleichwohl werden sie selten definiert. Eine Klärung beider Begriffe vor jeder Analyse ist daher unumgänglich. Es stellt sich jedoch die Frage, ob aufgrund des erwarteten Gegenübers überhaupt noch von Bedrohung und Verwundbarkeit gesprochen werden, oder Begriffe wie Risiko[6] nicht besser geeignet sind um das Problem analytisch zu durchdringen? Geht man davon aus, dass es eine Bedrohung durch Terroristen gibt (und das Wort Bedrohung angemessen ist), sollte versucht werden zu klären, welche Ziele Terroristen haben könnten.[7] Dadurch könnte sich die Chance ergeben, Objekte zu identifizieren, die als bedroht zu gelten haben. Anschließend ergibt sich die Frage, wie bestimmte Objekte geschützt werden können und ob der Schutz in einem klaren Kosten/Nutzen Verhältnis steht. Wie viele Ressourcen müssen investiert werden und was könnte der Preis sein, wenn diese Ressourcen nicht in eine, wie auch immer geartete, Vermeidung von Verwundbarkeit fließen?[8]

Neben diesen eher grundlegenden Fragen gilt es praktische, sich auch auf die aktuelle Politik beziehende, Fragen zu beantworten: Wie gefährdet sind Infrastrukturen[9] oder andere Einrichtungen durch unterschiedliche Arten von Angriffen? Was könnte bei einem Angriff

---

5 Im folgenden wird das Wort „substaatlichen Gruppen“ und „Terroristen“ synonym benutzt. Eine anerkannte Definition für Terroristen gibt es nicht. Die politische Verwendung des Begriffes „Terroristen“ ist nahezu beliebig und wird zu Propagandazwecken ebenso benutzt wie zur Diskriminierung oder zur Steigerung der Bedrohungsperzeption.

6 Vgl. Daase, Christopher / Feske, Susanne / Peters, Ingo (2002): *Internationale Risikoforschung: Ergebnisse und Perspektiven*, in: dies. (2002) (Hrsg.): *Internationale Risikopolitik. Der Umgang mit neuen Herausforderungen in den internationalen Beziehungen*, Nomos, S. 267 – 277.

7 Metzger, Jan (2004): *Das Konzept „Schutz kritischer Infrastrukturen“ hinterfragt*, in: Wenger, Andreas (Hrsg.): *Bulletin 2004 zur schweizerischen Sicherheitspolitik*, Zürich.

8 Als Beispiel drängt sich hier das US-amerikanische Raketenabwehr-Projekt auf. Die Kosten des Projektes steigen immer weiter an (es wird geschätzt, dass seit der Reagan-Ära ca. 130 Milliarden Dollar ausgegeben wurden) und es ist bis jetzt kein Einsatzdatum abzusehen. Welche Effekte könnten durch eine andere Investition des Geldes erreicht werden?

9 Infrastrukturen sind Einrichtungen wie das Transportnetz, die Wasserversorgung, Telekommunikationsnetze oder auch die Krankenversorgung. Eine genauere Definition von Infrastruktur erfolgt im Kapitel 1.c

passieren? Welches Schadenausmaß ist zu erwarten? Welche Regierungsstellen und wissenschaftliche Einrichtungen erstellen Studien über das Thema? Dieser und anderen Fragen werden in der folgenden Studie nachgegangen werden. Im ersten Kapitel werden ausgewählte Gefahrenaspekte und deren mögliche Konsequenzen beleuchtet werden. Anschließend folgt eine erste Zusammenfassung der bisherigen Reaktionen des deutschen Gesetzgebers sowie die Darstellung der wissenschaftlichen und öffentlichen Debatte. Vor dem Resümee folgt ein Ausblick auf bisherige Aktionen auf EU-Ebene in diesem Bereich.

1. Ausgewählte Gefahrenaspekte

Die unter anderem durch die Anschläge des 11. September 2001 heraufbeschworenen Anschlagsszenarien erstrecken sich auch auf Themenfelder wie den Einsatz von Massenvernichtungswaffen oder Angriffe auf die so genannten „Kritischen Infrastrukturen". Der 11. September hatte in seiner Wirkung tatsächlich Ausmaße angenommen, die auch mit kleinen Atombomben oder B-Waffen zu erreichen gewesen wären. Die Attentäter hatten eine „Massenvernichtung" ohne die Verwendung „klassischer" Massenvernichtungswaffen (MVW), also nuklearer, biologischer oder chemischer (NBC-)Waffen, erreicht. Flugzeuge wurden in „fliegende Kerosinbomben" verwandelt und gegen Ziele gesteuert, in denen sich viele Menschen aufhielten. In der Tat wurde von den Terroristen eine Schwelle überschritten, die die Terrorismusforschung als nicht wahrscheinlich angesehen hatte.[10] Dieses Tabu wurde gebrochen, was die Befürchtung nährt, dass in Zukunft substaatliche Akteure unkonventionelle, letale Substanzen biologischen oder chemischen Ursprungs nutzen könnten, um ihre Ziele zu erreichen.[11] Die Terror-Statistik zeigt, dass die Anzahl von Terroranschlägen abnimmt, dafür Einzelanschläge aber mehr Opfer fordern. Neben der Frage nach den potenziellen Möglichkeiten von Terrorangriffen mit MVW muss nach dem 11. September verstärkt auch die Frage nach den Motiven gestellt werden. Osama bin Laden hat einige Male auf ein Interesse an MVW hingewiesen und sogar behauptet, N- oder C-Waffen einsetzen zu wollen, wenn er darüber verfügen könnte.[12] Eine Auswertung der im Afghanistan-Krieg 2001/2002 gefundenen Dokumente zeigte jedoch keine wesentlichen Fortschritte.[13] Höchst beunruhigend ist jedoch die Meldung, zwei pakistanische Nuklearwissenschaftler hätten intensive Diskussionen mit Bin Laden u.a. bezüglich NBC-Waffen geführt. Dies belegt zumindest das Interesse von Terroristen an staatlichen Programmen zur Herstellung von Nuklearwaffen (NW). Auch tschetschenische Terroristen haben versucht, Nuklearanlagen anzugreifen bzw. radioaktives Material einzusetzen. Insgesamt halten sich Anschläge mit MVW durch Terroristen in Grenzen. Übersehen wird aber oft, dass vor dem Hintergrund des 11.9. Terrorattentäter auch konventionelle Waffen verwenden könnten, um Ziele anzugreifen, die NBC-Substanzen enthalten. Hier stellt sich die Frage, wie groß die nukleare oder biologische Sicherheit von Labors, Produktions- oder Lagerstätten gefährlicher Substanzen eigentlich ist. Zu unterscheiden ist also einerseits die

[10] Durch die Anschläge des 11. September ist der bisherige Leitsatz der Terrorismusforschung von Brian Jenkins „Terrorists want a lot of people watching, not a lot of people dead" widerlegt worden.

[11] Umfassende Studien findet sich u.a. bei Neuneck, Götz (1999): *Terrorism and Weapons of Mass Destruction - a New Symbiosis?* in: Klaus Gottstein (1999) (Hrsg.): *Proceedings of the XII International Amaldi Conference of Academies of Sciences and National Scientific Societies on Problems of Global Security*, Akademie der Wissenschaften in Mainz, Mainz 6.-9. Oktober 1999, S.296-323; Neuneck, Götz (2002): *Terrorismus und Massenvernichtungswaffen: Eine neue Symbiose?*, in: Hans Frank / Kai Hirschmann (2002) (Hrsg.): *Die weltweite Gefahr. Terrorismus als internationale Herausforderung*, Berlin-Verlag, S.169-224, S. 196.; Kelle, Alexander / Schaper, Anette (2001): *Bio- und Nuklearterrorismus. Eine kritische Analyse der Risiken nach dem 11. September*, HSFK-Report Nr. 10; Neuneck, Götz (2003): *Hype oder reale Gefahr: die Gefahr des Nuklearterrorismus zwei Jahre nach dem 11. September*, in: Informationsdienst Terrorismus, Nr. 2, S. 2 – 4

[12] Siehe dazu Neuneck, Terrorismus und Massenvernichtungswaffen, S. 196.

[13] Albright, David / Buehler, Kathryn / Higgins, Holly (2002): *Bin Laden and the bomb*, in: Bulletin of the Atomic Scientists, Jg. 58, Nr. 1, S. 23-25.

Verwendung vom MVW, die zu diesem Zweck selbst hergestellt oder gestohlen werden müssen und andererseits der Angriff mittels „konventioneller Munition“ wie Sprengstoff auf Ziele, die Substanzen (z.B. Chlor oder andere Industriegase) freisetzen, welche die Zerstörung oder Tötung vieler Menschen in Kauf nehmen. Die letztgenannte Strategie ist für Terroristen, die nicht in der Lage sind, die entsprechenden Substanzen selbst herzustellen, die „einfachere“ Vorgehensweise. Sie ist jedoch auch unberechenbarer.

A) Nuklear-Terrorismus

Führende Politiker, Organisationen und Fachleute warnten nach dem 11.09.2001 vor einem Einsatz von Nuklearwaffen (NW) und den Gefahren des Nuklearterrorismus (NT) durch „substaatliche Akteure“.[14] Der Grund liegt im Erbe des Kalten Krieges und des Atomzeitalters, in dem weltweit in Nuklearenergie investiert und enorme Mengen an Nuklearmaterial (Sprengköpfe, Reaktoren, Atommüll, Brennstofflager etc.) angehäuft wurden. Dieses Erbe istpotenzielles Ziel oder Quelle für die Abzweigung von waffenfähigem Material. Diverse Studien haben sich mit dem NT beschäftigt.[15] Ein Vergleich von NW mit biologischen und chemischen Waffen (B/CW) ergibt, dass diese bezogen auf die Schadenswirkung, die Möglichkeiten der Prävention und der Nachbehandlung eine eigene Kategorie bilden, die nicht mit dem riesigen Schaden einer Nuklearexplosion vergleichbarsind.[16] Ist eine Kettenreaktion erst in Gang gekommen, gibt es dagegen keine „Verteidigung“. Auch ist deutlich zu machen, dass die besagten „unkonventionellen Waffen“ sehr oft von Staaten in Auftrag gegeben und von Wissenschaftlern teilweise mit erheblichem Einsatz entwickelt wurden. Die heutigen MVW befinden sich im Besitz von Staaten, was folglich auch die Frage nach der Sicherheit dieser Arsenale bzw. die Gefahr der Weitergabe aufwirft. Dabei ist allerdings zu bedenken, dass „im allgemeinen“ Terroristen andere Ziele haben und eine andere Strategie verfolgen als Staaten, die sich MVW zulegen. Terroristen wollen in erster Linie Angst und Panik erzeugen, die Machtlosigkeit und Ohnmacht von Behörden und den Gesichtsverlust eines Staates erreichen.[17]

Bedrohungskategorien, Einsatzmöglichkeiten und Szenarien

Technisch sind prinzipiell vier Wege gangbar, um nukleare Schadenswirkungen zu erzielen:

1. Der Diebstahl oder die unerlaubte Weitergabe von *NW* oder *Komponenten*,
2. Der Bau improvisierter *nuklearer Sprengkörper*,
3. *Radiologische Waffen*,

---

[14] Siehe z.B. Pugwash Council (2001): *Pugwash Conferences on Science and World Affairs: The Dangers of Nuclear Terrorism. Statement of the Pugwash Council, Monday, 12 November 2001*, London.

[15] Siehe Georges Le Guelte (2002): *Le terrorisme nucléaire* , in : L'Année stratégique 2003, s/s dir. Pascal Boniface, Septembre 2002, pp. 75-84; Garwin, Richard (2002): *Nuclear and Biological Megaterrorism*, *presented at the 27th Session of the International Seminars on Planetary Emergencies, August 19-24*, New York; Maerli, Morten Bremer (2001): *Nuclear Terrorism Revisited*, in: Vierteljahresschrift Sicherheit und Frieden, Jg. 19, Nr. 4, S. 213-219; Maerli, Morten (2001): *The Threat of Nuclear Terrorism: Nuclear Weapons or other Nuclear Explosive Devices*, *Symposium of International Safeguards: Verification and Nuclear Material Security, 29 October -1. November*, Wien; Maerli, Morten (2002): *Terrorists and Crude Nuclear Devices*, *Pugwash Workshop No. 276*, Como (Italien).

[16] Ein detaillierter Vergleich findet sich in Neuneck, Terrorism and Weapons of Mass Destruction; Neuneck, Terrorismus und Massenvernichtungswaffen, S. 171 – 181. Harigel folgert: „Biological or chemical weapons used by any of those actors might be catastrophic locally, but relatively small compared with a nuclear holocaust. Again, a final judgement is still out.” Harigel, G. (2004): *Can terrorists acquire, produce, and use efficiently nuclear, radiological, chemical, or biological/toxin weapons?*, 9th PIIC Beijing Seminar on International Security, Nanjing/China 12-15 Oktober, 2004.

[17] Siehe dazu Waldmann, Peter (1998): *Terrorismus. Provokation der Macht*, Murman.

4. Angriffe auf *Nuklearanlagen.*

Die Optionen 1 und 2 können bei Überwindung der jeweiligen Schutz- und Sicherungsmaßnahmen und bei einem Diebstahl einer intakten NW zur Auslösung einer Kettenreaktion und damit zu einer verheerenden Atomexplosion führen; die Optionen 3 und 4 führen in erster Linie lediglich zu einer lokalen radioaktiven Verseuchung. Die beiden letzten Möglichkeiten sind leichter zu erreichen und für Terroristen durchaus realisierbar. Sie haben sicher keine militärische Bedeutung und passen gut zu den Zielen, die Terroristen haben, nämlich Aufmerksamkeit zu erzeugen. Um diese Optionen zu realisieren, sind verschiedene Wege denkbar:

Zum einen können *funktionsfähige Nuklearsprengköpfe*, die durch Staaten entwickelt worden sind, durch Diebstahl, illegalen Verkauf oder gewaltsame Entwendung in die Hände von Terroristen gelangen (Weg 1). Sorge muss hier der ungesicherte Status vorhandener Arsenale in Russland, sowie in Indien und Pakistan bereiten. Aber auch andere Nuklearstaaten sind nicht vollständig gegen Anschläge oder Diebstahl von waffenfähigem Material gefeit. Eine Studie der „National Academy of Science" sieht insbesondere in Russland und mittelfristig auch in Pakistan eine „signifikante Bedrohung" durch die Entwendung von funktionsfähigen Sprengköpfen.[18]

Der zweite Weg, eine Kettenreaktion auszulösen, besteht darin sich waffenfähiges Material zu besorgen, und einen einfachen, improvisierten Sprengsatz zu bauen und zur Explosion zu bringen. Das prinzipielle Wissen zum Bau einer Atombombe ist heute im Internet oder in entsprechender Fachliteratur frei verfügbar.[19] Unmittelbare Voraussetzung ist der Erwerb von Plutonium-239 (PU) oder hochangereichertem Uran (HEU). Zusätzlich sind Ingenieurkenntnisse nötig. Die kritische Masse liegt bei HEU je nach Anreicherungsgrad zwischen 6 und 30 kg oder mehr. Eine Plutonium-Bombe ist weitaus schwerer herzustellen als eine HEU-Bombe. Im letzteren Fall ist kein Test vonnöten, um das Funktionsprinzip auszuprobieren. Eine HEU-Bombe wäre auch für talentierte Spezialisten „machbar", wenn sie in den Besitz einer genügenden Menge von HEU gelangten. Lediglich zur Herstellung einer militärischen Nuklearwaffe wären mehrere Jahre Experimente unter dem Schutz eines Staates bei guter Ausstattung erforderlich. Entscheidend bleibt ein schneller Zugriff auf HEU (oder PU): Wenn HEU vorhanden ist, reduziert sich die benötigte Zeit auf Monate, Wochen oder Tage.[20] NW-Designer haben bestätigt, dass sich mit HEU nach dem „Kanonenprinzip" auch durch Nichtfachleute eine Kettenreaktion auslösen lässt. Deutlich wird hier, dass die Sicherheit von waffenfähigem Material, insbesondere PU und HEU, entscheidend ist. Ist das Material erst einmal aus Lagerstätten verschwunden, ist es schwer wiederzubeschaffen und kann folglich durch Weitergabe auch in Terroristenhand geraten und für eine Kettenreaktion mit unübersehbaren Folgen missbraucht werden.

Der dritte Weg, welcher der Kategorie „Nuklearterrorismus" zugerechnet wird, ist die Fabrikation und der Einsatz einer *radiologischen Waffe* (Radiological Dispersal Device, RDD).[21] Hier müssen in geeigneter Weise radioaktive Materialien mit einem Sprengstoff kombiniert und danach zur Explosion gebracht werden. Eine Kettenreaktion kommt nicht zustande, und die anschließenden Wirkungen sind abhängig von der Art der Verbreitung, den lokalen Umweltbedingungen, der Frühwarnung etc. Das größte Sicherheitsproblem hier liegt

---

18 National Research Council (2002): *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*, The National Academies Press, http://www.nap.edu/catalog/10415.html (07.07.2005), S. 43ff.

19 Robert Serber (1992): *The Los Alamos Primer, The First Lectures on How To Build An Atomic Bomb*, Berkeley.

20 Auch ein schneller Zusammenbau einer „primitiven Waffe" vor Ort ist im Prinzip denkbar. Hier müsste lediglich das Wachpersonal entsprechender Einrichtungen überwältigt werden, um an das waffenfähige Material zu gelangen und es zu einem Sprengsatz zusammenzusetzen.

21 Siehe z.B. U.S. Nuclear Regulatory Commission: *Fact Sheet on Dirty Bombs*, http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/dirty-bombs.html (05.07.2005).

darin, dass es radioaktives Material für viele medizinische, industrielle und wissenschaftliche Anwendungen gibt.[22] Forschungsanlagen, Kliniken, Fabriken und Nuklearanlagen, die über radioaktives Material verfügen, sind in Deutschland unterschiedlich geschützt (von Randow 2002). In Deutschland werden pro Jahr 800.000 Sendungen mit radioaktivem Inhalt befördert. Die radioaktiven Quellen sind unterschiedlich groß und unterschiedlich klassifiziert bzw. gesichert. Ein CIA-Report vom 23.11.2004 geht davon aus, dass Al-Qaida Interesse am Bau einer „schmutzigen Bombe" hatte und ihr Bau im Rahmen der Möglichkeiten der Organisation liegen. Eine Modellrechnungen zur Freisetzung von Kilogrammmengen Cäsium und Plutonium zeigen, dass große Gebiete für längere Zeit unbewohnbar gemacht werden würden.[23] Eine Dekontaminierung alleine reicht möglicherweise nicht, ein Abtragen des Bodens oder der Häuseraußenfläche könnte nötig werden, wenn die Dekontamination nicht schnell genug erfolgt. In Deutschland befindet sich eine Melde- und Alarmzentrale im Aufbau. Die Website des Deutschen Notfallvorsorge-Informationssystem-DENIS[24] bietet zwar einige Informationen (Schlagworte, Länderdaten etc.) an, eine ausfeilte Organisationsstruktur und bundesweite Notfallpläne scheint es vor dem Hintergrund unterschiedlicher Behörden- und Länderkompetenzen nicht zu geben. Ein Artikel der Frankfurter Allgemeinen Zeitung von 2002 geht davon aus, dass die Behörden nur „ungenügend" vorbereitet sind. Eine Simulationsübung in Dänemark ergab, dass Dänemark über keinen nationalen Notfallplan oder geeignetes Krisenmanagement verfügt.[25] Es bliebe zu prüfen, ob dies für ganz Europa gilt und welche Rolle die EU hier in Zukunft übernehmen kann. Die IAEO hat in den letzten Jahren technische Standards zur Kategorisierung und Meldung radioaktiver Quellen sowie einen „Code of Conduct for Safety and Security of Radioactive Sources" ausgearbeitet. Angesichts durchlässiger Grenzen innerhalb und außerhalb der EU und der speziellen Expertise zur Vorbeugung und Schadensbewältigung bei RDD-Anschlägen sollte die EU ein europaweites Krisenmanagement errichten.

Die vierte Möglichkeit, die dem NT zuzurechnen ist, wäre *ein Angriff auf zivile Nuklearanlagen*, der so wirkungsvoll ist, dass dort lagerndes Nuklearmaterial freigesetzt wird. Mögliche Ziele wären hier Kernkraftwerke (KKW), Abklingbecken, Zwischenlager (in Deutschland befinden sich diese auf dem Gebiet von KKWs) oder Wiederaufarbeitungsanlagen. Allgemein ist bekannt, dass deutsche KKW zum Teil gegen Kampfjets, nicht jedoch gegen größere Passagiermaschinen, die gezielt auf einen Reaktor zum Absturz gebracht werden, gehärtet sind. Weitergehende Analysen und Modellrechnungen sind nötig, um künftige „Terrorszenarien" abzudecken. In den USA wird dies von der Nuclear Regulatory Commission (NRC), dem Sandia-Labor und der Zivilindustrie durchgeführt.[26] Diskutiert wird auch die Frage, welchen „Erfolg" Angriffe durch Terroristen auf Abklingbecken oder Transportbehälter haben könnten. Klar ist, dass der „Erfolg" eines Angriffs von dem Design des KKWs und der Größe und „Professionalität" des Angriffs abhängt. In Deutschland wurden im Auftrag des Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit (BMU) Untersuchungen durch die „Gesellschaft für Reaktorsicherheit" (GRS) unternommen. Es wurden fünf Gruppen von Anlagen auf ihre „Verwundbarkeit" hin untersucht. Dabei wurden neun Schadensszenarien zugrunde gelegt und die

[22] Weltweit gibt es Millionen von radioaktiven Quellen, die meisten von ihnen sind jedoch nur schwach radioaktiv. Siehe dazu: International Atomic Energy Agency (IAEA) (2005): *Inadequate Control of World's Radioactive Sources*, http://www.iaea.org/NewsCenter/Features/RadSources/rads_factsheet.pdf (05.07.2005).

[23] Kelly, Henry (2002): *Testimony of Dr. Henry Kelly before the Senate Committee on Foreign Relations*, March 6 2002, http://www.fas.org/ssp/docs/030602-kellytestimony.htm (05.07.2005).

[24] www.denis.bund.de

[25] Dalgaard-Nielsen, Anja / Selmer-Friborg, Line / Jakobson, Martin (2005): *Targeting Europe: The Threat from Dirty Bombs*, Danish Institute for International Studies, http://www.diis.dk/sw8793.asp (05.07.2005).

[26] Garwin, Richard (2002): *Nuclear Power Plants and Their Fuel as Terrorist Targets*, in: Science, 20 September 2002, S. 1997, 1999.

„Beherrschbarkeit“ der jeweiligen Szenarien eruiert.[27] Potenzielle Ziele sind selbstverständlich nicht nur KKW in Deutschland, sondern auch in anderen Ländern der EU. Des Weiteren wurden konkrete Schutzmaßnahmen gegen gelenkte Flugzeugangriffe auf deutsche KKW vorgeschlagen (Einnebeln der KKW, Sperrmauern etc. siehe Kap.3).

Sicherheit von Nuklearmaterial und mögliche Quellen

Entscheidend dürfte sein, inwieweit es substaatlichen Akteuren gelingt, in den Besitz von waffenfähigem Material zu kommen. Wichtig ist also, die Sicherheit der waffenfähigen Arsenale der Großmächte USA und Russland, aber auch der Arsenale kleinerer Nuklearmächte, zu gewährleisten.[28] Da HEU besonders für terroristische Zwecke geeignet ist, sollte dieses Material unbedingt mit niedrig angereichertem Uran vermischt und somit „downgeblendet“ werden. Leider ist dies bisher nur in geringem Maße geschehen und Spielball ökonomischer Interessen.[29] Eine Studie für das schwedische Außenministerium weist auf die Dringlichkeit der Problematik hin und erarbeitet Alternativen.[30]

Die Hauptsorge bezüglich globaler nuklearer Sicherheit muss sicherlich dem russischen Nuklearkomplex gelten.[31] Bezüglich der Lagerorte, des Standes der Sicherheitssysteme und der Moral der Wachmannschaften gibt es umfangreiche Literatur, die zeigt, wie prekär die Situation ist. Die Nuklearstatistik des Bundeskriminalamtes (BKA) bzw. der IAEO verzeichnet zwar eine Abnahme der Fälle von Nuklearschmuggel mit spaltbarem Material, dafür steigt die Zahl der Zwischenfälle mit radioaktiven Quellen stark an. Diese Statistik sagt jedoch nur etwas über den Misserfolg von Nuklearschmuggel aus, nichts jedoch über gelungene Versuche, die man nicht hat verhindern können. Wesentlich sind natürlich zudem die Materialmengen, die geschmuggelt wurden. Darüber gibt die Datenbank der Stanford University näher Auskunft. Laut der Stanford-Datenbank wurde 1992-2002 eine Gesamtmenge von 39 kg waffenfähigen Materials (HEU und Pu) weltweit beschlagnahmt. Besondere Aufmerksamkeit muss auch der „Verwundbarkeit von Forschungsreaktoren“ gewidmet werden.[32] Die Diebstahlfälle bei Forschungsreaktoren deuten darauf hin, dass diese unzureichend geschützt sind, obwohl das Inventar dieser Reaktoren geringer als das von Leistungsreaktoren ist. Eine Harvard Studie von 2003 kommt vor diesem Hintergrund zu dem Ergebnis: “[the] *United States and its partners must do everything in their power to ensure that every nuclear weapon, and every kilogram of HEU and plutonium, wherever it may be in the world, is secure and accounted for, to stringent standards*.”[33]

Aufgrund der bisherigen Aussagen lassen sich einige *Schlussfolgerungen* ziehen. Für substaatliche Akteure ist es durchaus möglich, mit geringem Aufwand einen einfachen

---

27 Siehe Bundesamt für Umwelt, Naturschutz und Reaktorsicherheit (2002): *Schutz der deutschen Kernkraftwerke vor dem Hintergrund der terroristischen Anschläge in den USA vom 11. September 2001*, Bonn 27.11.2002, http://www.bund.net/lab/reddot2/pdf/grs_gutachten.pdf (05.07.2005).

28 Alleine Russland verfügt über schätzungsweise mehr als 1.000 Tonnen HEU, von denen lediglich die Hälfte als überschüssig deklariert wurde, die USA verfügen über 645 Tonnen.

29 Calogero, Francesco (1997): *Fast-track the uranium deal*, Bulletin of the Atomic Scientists, Jg. 53, Nr. 6, S. 20-21. Ders. (1998): *Reply to letter*, Bulletin of the Atomic Scientists, Jg. 54, Nr. 1, S. 66.

30 Eliminating Stockpiles of Highly Enriched Uranium -- Options for an Action Agenda in Cooperation with the Russian Federation*, Report to be submitted to the Swedish Ministry for Foreign Affairs by the HEU Elimination Expert Group, 2003.*

31 Siehe z.B. Neuneck, Terrorismus und Massenvernichtungswaffen, S. 197-204; Matthew Bunn: The next wave: Urgently needed new steps to arms control warheads and fissilel materials, April 2000. Bunn, Matthew (2000): *The Next Wave. Urgently Needed New Steps to Control Warheads and Fissile Material*, Harvard University´s Project on Managing the Atom and the Non-Proliferation Project of the Carmnegie Endowment for International peace.

32 Siehe dazu Bunn, G. / Braun, C. / Glaser, A. / Lyman, E. / Steinhausler, F. (im Erscheinen): *Research Reactor Vulnerability to Terrorists: An Unrecognized Peril in Need of Urgent Attention*, Science and Global Security.

33 Bunn, Matthew / Wier, Anthony /.Holdren, John (2003): *Controlling Nuclear Warheads and Materials, A Report Card and Action Plan*, Nuclear Threat Initiative (12. März 2003), http://www.nti.org/e_research/cnwm/overview/report.asp (05.07.2005).

Nuklearsprengkörper mit HEU als Ausgangsmaterial zu erlangen. Die Anstrengungen, PU oder HEU herzustellen, liegen über den Kapazitäten von Einzelpersonen oder Gruppen, es sei denn, sie werden durch einen Staat gestützt und können unbehelligt und materiell gut ausgestattet an der Produktion von Nuklearmaterial arbeiten. Die heutigen enormen Arsenale an waffenfähigem Material sind in den Händen der acht bekannten NW-Staaten. Darüber hinaus befinden sich radioaktive Anlagen und Quellen in allen Staaten, die über eine Nuklearindustrie verfügen. Letztere könnten das Ziel von Terroranschlägen werden. Die Sicherung und die Reduktion von NW und Nuklearmaterial (NM) muss deshalb höchste Priorität haben. Besonders der Verringerung der HEU-Bestände in Russland muss höchste Dringlichkeit eingeräumt werden. Ist das Material erst einmal entwendet, ist es kaum mehr kontrollierbar.[34] Somit hängen nukleare Sicherheit, Abrüstung und Rüstungskontrolle und NT unmittelbar zusammen. Dies gilt nicht nur für die klassischen Nuklearmächte, sondern auch für Pakistan, wo die Sicherheit von nuklearwaffenfähigem Material besorgniserregend ist. Dennoch ist eine mehrstufige Abwehr, beginnend bei frühzeitiger Aufklärung entsprechender Akteure und Ziele, ebenso notwendig wie die Einübung und Koordination eines effizienten Katastrophenmanagements und der Installation von Radioaktivitätsmeldern in Häfen, Grenzstationen und auf Flugplätzen. Insbesondere Häfen könnten Primärziele für terroristische Anschläge mit MVW sein. Ein Anschlag in einer Hafenstadt kann nicht nur tausende Menschen töten, sondern auch den Handelsverkehr für längere Zeit unterbrechen.[35]

Den Abrüstungs- und Sicherungsinitiativen der USA, EU, UN und NATO kommt eine entscheidende Bedeutung zu. Allerdings gibt es hier bürokratische Hindernisse, die die Umsetzung sehr verlangsamen. Die internationale Gemeinschaft hat in den letzten Jahren diverse Aktionen, Konventionen und Initiativen in diese Richtung gestartet, deren Effizienz angesichts des Problems aber offen ist. Zu nennen ist hier die G-8 Initiative „Global Partnership“. Schwerpunkte sind hier:

1. Sicherung der Sprengköpfe und des Materials,
2. Abfangen von Nuklearschmuggel,
3. Stabilisierung der Arbeitsbedingungen von Nuklearpersonal,
4. Monitoring der Arsenale bzw. Reduktionen,
5. Beendigung der Produktion waffenfähigen Materials,
6. Reduktion überschüssigen Materials.

Die Initiative bildet einen ersten wichtigen Schritt, dennoch reichen die bisher eingesetzten finanziellen und technischen Mittel bei weitem nicht aus.[36] Zum einen ist die Umsetzungsgeschwindigkeit recht langsam, zum anderen ist fraglich, ob das investierte Geld effizient eingesetzt wird. Eine gründliche Untersuchung der Harvard-Universität (2003) im Auftrag der „Nuclear Threat Initiative“[37] kommt zu dem Schluss, dass in Russland bisher lediglich 100 Tonnen des waffenfähigen Materials, das sich außerhalb von NW befindet, „umfassend gesichert“ wurden, während 122 Tonnen „vorläufig“ und 378 Tonnen noch gar nicht „gesichert“ wurden.

---

34 Erinnert sei an das Demonstrationsexperiment von ABC News / NRDC vom September 2002, bei dem eine für eine einfache Atombombe genügende Menge (abgereicherten) Urans in einem Container in die USA eingeführt und nicht gefunden wurde, obwohl der Container inspiziert wurde. Siehe dazu Christopher Paine (2002): *Preventing Nuclear Terrorism. Testimony to the House Committee on Government Reform*, Subcommittee on National Security, Veterans Affairs, and International Relations, 107th Congress, 2nd Session, September 24 2002.

35 Im Jahr 2001 erreichten 5,7 Millionen Container die USA-Häfen, dabei werden jedoch nur 2 Prozent inspiziert. Siehe Medalia, Jonathan. (2003): *Terrorist Nuclear Attacks on Seaports: Threat and Response*, CRS Report for Congress, 13. August 2003, Washington D.C.

36 Siehe hierzu umfassend eine erste Einschätzung von Einhorn, Robert J. / Fluornoy, Michèle (Hrsg.) (2003): *Protecting Against the Spread of Nuclear, Biological, and Chemical Weapons: An Action Agenda for the Global Partnership (4 Vols.)*, Center for Strategic and International Studies, Washington, D.C.

37 Bunn et al., Controlling Nuclear Warheads, S. 78ff.

Weiterführende Forschungsfragen

- Wie ist lässt sich die Effizienz der Programme zur Sicherung des waffenfähigen Materials besonders im Bereich der ehem. Sowjetunion erhöhen?
- Wie sicher ist die nukleare Infrastruktur in Deutschland und Europa?
- Welche Anschlagsszenarien mit radiologischen Waffen sind denkbar?
- Welche Kontrollen an Schlüsselpunkten sind heute durchführbar?

B) Bedrohung durch biologische und chemische Substanzen

Die Diskussion von Sicherheitsbedrohungen durch biologische Agenzien reicht heute von der Ausbreitung ansteckender Krankheiten (SARS, Ebola, Pocken) über mögliche Folgen wissenschaftlicher Experimente (modifizierter Mauspockenerreger, Biowaffentests) bis hin zu bioterroristischen Anschlägen oder Akten biologischer Kriegführung durch Staaten. So folgert ein kürzlich veröffentlichter Bericht einer internationalen Konferenz der nationalen Akademien der Wissenschaften: „Unsere Gesellschaften seien potentiell verwundbar geworden durch künstlich erzeugte Viren (Rekonstruktion des Grippevirus von 1918), Laborunfälle, durch Botulismus bei der Nahrungsmittelproduktion und durch Anthrax- und Giftanschläge durch Psychopathen und Kriminelle."[38]

B-Waffen[39] sind krankheitsverursachende Mikroorganismen wie Bakterien, Ricketsien oder Viren. Bestimmte Bakterien werden auch verwendet, um hochgiftige Toxine zu produzieren. *Biologische Agenzien* sind bezogen auf die Letalität pro Masse weitaus tödlicher als NW. Sowohl bei der Herstellung als auch beim Einsatz unterscheiden sich BW stark in Bezug auf das Epidemierisiko, die Infektivität, die Stabilität, die Lebensdauer und die Retroaktivität.[40] Die meisten Agenzien, die für BW-Kriegsführung in Betracht kommen, sind infektiös, aber selten ansteckend. Viele B-Waffen (Anthrax, Pest, Botulinus) sind gegenüber ungeschützten Personen höchst tödlich, wenn sie als Aerosol in die Lunge der Opfer gelangen. Andererseits können schnell durchgeführte Schutzimpfungen die Todesraten stark senken. Da die Inkubationszeit in vielen Fällen ein paar Tage beträgt, ist es schwierig, den Verursacher dingfest zu machen. Andererseits besteht die Gefahr, dass die infizierte Person sich in Unkenntnis der Ansteckung über große Entfernungen bewegt und Epidemien auslöst. Dies ist im Falle einer Ausbreitung von Pocken besonders gefährlich. BW sind geruchlos und für das menschliche Auge nicht sichtbar. Eine Detektion ist schwierig und abhängig von der Art des Angriffs und der Qualität des jeweiligen Gesundheitssystems. BW können theoretisch große Opferzahlen verursachen, ihre realen Wirkungen sind im praktischen Einsatz jedoch schwer zu bestimmen. Um ähnliche tödliche Wirkungen mit chemischen Waffen hervorzurufen, sind – insbesondere im Freien – weitaus größere Substanzmengen nötig.[41]

Einige Aufsehen erregende Ereignisse haben das Problem der BW in das Zentrum der Diskussion gerückt. Die UdSSR betrieb ein umfassendes B-Waffen-Programm, das zwischen 1989 und 1992 schrittweise offenbart wurde. Die UN „Special Commission" (UNSCOM) entdeckte 1995, dass der Irak seit 1974 ebenfalls an BW-relevanten Materialien arbeitete. Zwischen 1987 und 1991 wurden größere Mengen an BW-Agenzien angelegt und

---

38 Eisenbart, C. / Gottstein, K. / Häckel, E. / Kelle, A. / Matz, N. / Neuneck, G. / Wolthusen, S. (2004): *Konferenzbericht*, XVI International Amaldi on Problems of Global Security, Triest, 18.-20. November 2004.

39 Siehe dazu ausführlich: Tucker, Jonathan (Hrsg.) (2000): *Toxic Terror. Assessing Terrorist. Use of Chemical and Biological Weapons*, MA Press; Leitenberg, Milton (2004): *The Problem of Biological Weapons*, The Swedish National Defense College.

40 Siehe dazu Nixdorff, K. / Hellmich N. / Matousek, J.: *B- und C-Waffen Potenziale und die Gefahr eines Einsatzes durch Terroristen*, in: Wissenschaft und Frieden 2003-4, Dossier Nr. 44.

41 Ein Vergleich findet sich in Neuneck, Terrorismus und Massenvernichtungswaffen, eine neuere Analyse bei Nixdorff et al., B- und C-Waffen Potenziale.

Trägersysteme zur Ausbringung dieser tödlichen Substanzen vorgesehen.[42] 1995 verübten Mitglieder der Aum-Sekte in Japan mit Nervengas Anschläge in der Tokioter U-Bahn. Bei den nachfolgenden Untersuchungen stellte sich heraus, dass Aum-Mitglieder auch an der Herstellung und Ausbringung – allerdings erfolglos – an gefährlichen Pathogenen arbeiteten.

In den USA beschloss schon die Clinton-Administration ein umfangreiches Schutz-Programm.[43] In Deutschland findet die Diskussion meist in Expertenkreisen statt, hat seit 2001 aber auch verstärkt politische Hintergründe.[44] Das Wissens um die Ausrüstung zur Herstellung von tödlichen Substanzen ist heute sicher weiter verbreitet als noch vor zehn Jahren. Die wissenschaftlichen Fortschritte auf dem Gebiet der Gen- und Biotechnologie lassen Experten zudem befürchten, dass der Einsatz von BW und die Erzeugung neuerer Agenzien wahrscheinlicher werden. Nixdorff et al.[45] folgern allerdings: „Es ist jedoch unwahrscheinlich, dass substaatliche Terroristen die oben genannten Manipulationen für die Herstellung neuartiger Mikroorganismen in der nahen Zukunft anwenden werden bzw. können." Die Zahl der Anschläge mit B- und CW ist bisher sehr klein und die Zahl der Opfer recht gering. Es gibt vier nennenswerte Fälle für deren Einsatz durch substaatliche Akteure: Bei den Salmonellenvergiftungen der Rajneeshee-Sekte 1984 waren keine Opfer zu beklagen. Bei zwei Anschlägen (1990 und 1995) wurden Chemikalien (Chlorgas und Sarin-Nervengas) eingesetzt und es starben in Japan 13 Menschen. Die Anthrax-Anschläge 2001 verursachten fünf Tote. Vieles deutet darauf hin, dass der Anthrax-Stamm von einem Fachmann aus einem Waffenlabor hergestellt wurde. Die Zahl der Beschaffungsfälle oder des gescheiterten Einsatzes liegt zwar höher, zeigt aber, dass ihr Einsatz nicht so trivial ist wie oft angenommen. Erwiesen ist auch, dass Al Qaeda-Angehörige mit Chemikalien (Zyanid, Industriechemikalien) in geschlossenen Räumen experimentierten, die relativ leicht zu beschaffen sind. In Bezug auf B-Waffen muss gefolgert werden, dass zu ihrer Herstellung sehr spezifische Kenntnisse erforderlich sind, die nur von Insidern und Angestellten kritischer biologischer Labore stammen können. Angesichts der Letalität und des Infektionsrisikos mancher Substanzen muss man dennoch von einem Risiko mit geringer Eintrittswahrscheinlichkeit aber einem hohen Schadenspotenzial sprechen. Insbesondere Waffenlabors sowie Staaten, die heimlich B-Waffen-Forschung betreiben bzw. betrieben haben, sind eine mögliche Quelle.

Auch beim Bio- und C-Waffenterrorismus gilt, dass ein Bündel von Maßnahmen vorbeugend wirken kann. Dies kann von der Austrocknung von Finanzquellen, Verbesserung der Personenkontrollen und der Detektion von relevantem Material bis hin zur Verbesserung der völkerrechtsrelevanten Normen reichen. Das B-Waffenübereinkommen (BWÜ) von 1972 verbietet im Prinzip eine ganze Kategorie von MVW und zwar die biologischen Wirkstoffe und Toxine. Das Übereinkommen trat 1975 in Kraft, inzwischen haben es 153 Staaten von 169 Unterzeichnern ratifiziert. Ein großes Problem ist, dass es im Rahmen des BWÜ bisher nicht gelungen ist, ein effektives Verifikationsprotokoll inklusive einer dafür zuständigen Organisation zu etablieren oder zu verabschieden um ein mit der C-Waffenkonvention vergleichbares Überprüfungsregime aufzubauen. Auch bei der Überprüfungskonferenz 2001 gelang es nicht, ein Verifikationsprotokoll zu verabschieden.[46] Die US-Regierung begründet ihre ablehnende Haltung damit, dass das Protokoll ineffektiv sei und den nationalen Interessen der USA widerspreche. Dies bedeutet aber auch, dass staatliche Labors generell nicht überwacht werden.

Einige NGOs haben deshalb eigene Vorschläge erarbeitet. Das Harvard-Sussex-

---

42 Siehe Tucker, Toxic Terror; Leitenberg, The Problem of Biological Weapons.

43 Tucker, The Future of Armed Resistance; Neuneck, Terrorism and Weapons of Mass Destruction,; Neuneck, Terrorismus und Massenvernichtungswaffen, S. 193ff.

44 So bemängelt die Opposition, dass zu wenig für den B-Waffenschutz durch die rot-grüne Regierung getan wird.

45 B- und C-Waffen Potenziale

46 Siehe dazu Kelle / Schaper, Bio- und Nuklearterrorismus, S.12ff.

Program schlägt vor im Rahmen einer „Draft Convention to Prohibit Biological and Chemical Weapons under International Criminal Law", die Entwicklung, Herstellung, Lagerung, Erwerbung, Zurückhaltung und Verwendung von B/CW einem internationalen Verbrechen gleichzustellen. Das „BioWeapons Prevention Project" (BWPP) will durch Monitoring, Reports und Networking die Normen gegen „Krankheiten als Waffe" stärken.[47] Das Internationale Komitee vom Roten Kreuz (ICRC) startete die Initiative „Biotechnology, Weapons and Humanity" und schlägt die Schaffung eines „web of prevention" vor, um den Missbrauch von Biotechnologie zu verhüten.[48] Die britische Royal Society hat in einer Studie Maßnahmen ausgearbeitet, wie im Bereich Forschung und Entwicklung (F&E) der Missbrauch oder der kriminelle Gebrauch von Biotechnologie zu verhindern sei.[49] Die internationale Debatte steckt hier aber noch in den Kinderschuhen. Bei den chemischen Waffen hat die Organisation für das Verbot chemischer Waffen (erfolglos versucht, in einen Dialog mit Chemieverbänden über die ethische Dimension der Aktivitäten zu treten.

Angesichts der Tatsache, dass gefährliche Bioagenzien Grenzen durch Schmuggel ungehindert überwinden bzw. mögliche Epidemien vor Grenzen nicht Halt machen, müssten Gefahrenabwehr und wirkungsvolles Katastrophenmanagement international koordiniert werden. Internationale Organisationen (WHO, UN, OECD etc.) bzw. überstaatliche Entitäten wie die EU sollten hier eine zentrale Rolle spielen. Diese könnte von der Schaffung einheitlicher Gesundheitsrichtlinien oder von Hilfsprogrammen für von Epidemien betroffene Staaten bis hin zu Impf- und Trainingsprogrammen des betroffenen Personals reichen.

Weiterführende Forschungsfragen

- Wie gut sind biologische Forschungsstätten vor gewaltsame Übergriffen geschützt?
- Wie können Innentäter und Kriminelle vom Einsatz gefährlicher Substanzen abgehalten werden?
- Wie sicher sind Lagerstätten chemischer Waffen gegenüber gewaltsamen Übergriffen?

C) Schutz Kritischer Infrastrukturen

> „I mean virtually every vital service – water supply, transportation, energy, banking and finance, telecommunications, public health. All of these rely upon computers and the fiber-optic lines, switchers and routers that connect them. Corrupt those networks, and you disrupt the nation. It is a paradox of our times: the very technology that makes our economy so dynamic and our military forces so dominating – also makes us more vulnerable." (Condolezza Rice 2001)

Obwohl das angeführte Zitat der ehemaligen US-amerikanischen Sicherheitsberaterin und jetzigen Außenministerin Condolezza Rice auf die USA zugeschnitten ist, beschreibt es doch auch die Problematik Kritischer Infrastrukturen in anderen entwickelten Industrienationen wie Deutschland. Im Kern wird angenommen, dass eine Gesellschaft bestimmte Infrastrukturen zur Funktionsfähigkeit braucht, sowohl in wirtschaftlicher als auch in militärischer und gesamt gesellschaftlicher Hinsicht. Die Abhängigkeit von diesen Infrastrukturen führt nach

[47] Vergleiche www.bwpp.org (05.07.2005)
[48] Vgl. ICRC (2004): *Biotechnology, Weapons and Humanity: Introduction*, http://www.icrc.org/Web/eng/siteeng0.nsf/html/5VDJ7S (05.07.2005)
[49] The Royal Society (2004): *Do no harm: reducing the potential for misuse of life science research*, http://www.royalsoc.ac.uk/document.asp?id=2830&printer=1 (05.07.2005)

Ansicht von Experten[50] dazu, dass Industrienationen besonders empfindlich gegenüber Angriffen auf diese sind.

Die Verwundbarkeit der Gesellschaft durch Angriffe auf Kritische Infrastrukturen wurde von skandinavischen Staaten schon während des Kalten Krieges analysiert (Dunn/Wigert 2004). Die Diskussion begann in den USA mit der Einsetzung der „*Presidential Commission on Critical Infrastructure Protection"* (PCCIP) durch den damaligen Präsidenten Clinton. Die Kommission legte 1997 ihren Abschlussbericht[51] vor, in dem sie die Abhängigkeit und Verwundbarkeit von acht unterschiedlichen Infrastrukturen[52] betrachtete. Eines der Ergebnisse der PCCIP ist, dass Computertechnologie die Infrastrukturen noch enger verbunden und damit noch anfälliger für Störungen gemacht hat.[53] In Deutschland wurde, unter anderem als Reaktion auf die Entwicklungen in den USA[54], die Arbeitsgemeinschaft Kritische Infrastrukturen (AG KRITIS) unter Federführung des Bundesministerium des Inneren eingesetzt. Die AG KRITIS hatte als erste Aufgabe einen Bericht zu erstellen, der zum Ziel hatte, Bedrohungsszenarien zu entwerfen und Schwachstellen der über Informationssysteme angreifbaren Systeme zu ermitteln, sowie Möglichkeiten zur Behebung der Schwachstellen oder zumindest einer Minderung der zu erwartenden Schäden auszuarbeiten sowie Vorschläge zu einem Frühwarn- oder Analysesystem zu entwickeln.[55] Die Endversion des Berichtes ist nicht veröffentlich worden, allerdings kursiert im Internet ein Vorabbericht: Ergebnisse der Kommission sind:

- Erfahrungen der USA lassen sich nicht einfach auf Deutschland übertragen.
- Die Gefährdung durch andere Akteure ist nicht sehr hoch, allerdings können sehr schnell Änderungen eintreten.
- Sicherheitsstrategien sollten sich auf defensive Maßnahmen konzentrieren.
- Es sollte eine Optimierung der umfassenden Gewinnung von Schwachstellenanalysen vorgenommen werden.
- Manipulationen von Kritischen Infrastrukturen werden wahrscheinlich auf elektronischem Wege erfolgen.
- Es müssen angepasste Schutzstrategien für Hochverfügbarkeitssysteme entwickelt werden.

Die Kategorisierung kritischer Strukturen variiert nicht nur zwischen Staaten sondern auch über die Zeit. So behandelte die PCCIP sieben unterschiedliche Strukturen, regte aber die Aufnahme weiterer an. Inzwischen ist die Anzahl der Kritischen Infrastrukturen auf 13[56] angewachsen. In Deutschland hingegen werden acht[57] Infrastrukturen als kritisch für den Staat betrachtet.[58] Trotz der Unterschiede kann davon ausgegangen werden, dass es einen Kernbereich an Kritischen Infrastrukturen gibt, der für alle Staaten gleich ist und einen

---

50 Schörnig, Niklas (2001): *Demokratischer Frieden durch überlegene Feuerkraft*, HSFK-Standpunkte Nr. 3/2001, S. 6.

51 Presidential Commission on Critical Infrastructure Protection (1997): *Critical Foundations -Protecting America's Infrastructures*, http://www.tsa.gov/public/interweb/assetlibrary/Infrastructure.pdf (08.06.2004).

52 Telekommunikation, Elektrizität, Gas und Öl Lagerung und Transport, Bank- und Finanzwesen, Transportwesen, Wasserversorgung, Notfallversorgung und Regierungsdienstleistungen.

53 PCCIP, Critical Foundations, S. 4

54 Stein, Willi / Ritter, Stefan (2003): *Schutz Kritischer Infrastrukturen – Aktivitäten in Deutschland*, in <kes> – Die Zeitschrift für Informations-Sicherheit, 2003(4), S. 41-44, S. 42.

55 KRITIS (1999*): Informationstechnische Bedrohungen für Kritische Infrastrukturen in Deutschland*, http://userpage.fu-berlin.de/~bendrath/Kritis-12-1999.html (15.12.2004), 7/24.

56 Die „National Strategy For Homeland Security" führt folgende Bereiche als kritisch auf: Landwirtschaft, Lebensmittel, Wasser, Notfalldienste, Rgeirung, Miltärisch.Industrielle Basis, Information und telekommunikation, Energie, Transportwesen, Banken und Finanzen, Chemische Industrie, Post- und Versandwesen und die öffentliche Gesundheitsversorgung.

57 Transport und Verkehr; Energie, Gefahrenstoffe; Informationstechnik und Telekommunikation; Finanz-, Geld und Versicherungswesen; Behörden, Verwaltung und Justiz; Sonstiges (Medien, Großforschungseinrichtungen sowie herausragende oder symbolträchtige Bauwerke, Kulturgut)

58 Stein, Willi (2004): *Critical Infrastructure Protection (CIP) - A Sector-oriented Introduction*, Beitrag zur Konferenz: CRITICAL INFRASTRUCTURE PROTECTION AND CIVIL EMERGENCY PLANNING, Dependable Structures, Cybersecurity and Common Standards, 9.-11. September 2004, Zürich.

erweiterten Bereich, der zwischen den Staaten variiert. Das Kernfeld umfasst die Infrastrukturen Verkehr, Energie, Information und Kommunikation, Finanzdienstleistungen, Regierungsdienstleistungen und Notfallversorgung.

Inzwischen beschäftigen sich unterschiedliche Stellen mit dem Schutz Kritischer Infrastrukturen, zumeist unter Führung des Bundesministerium des Innern (BMI). Hervorzuheben sind hier ein Referat[59] im Bundesamt für Sicherheit in der Informationstechnik (BSI), welches sich hauptsächlich mit dem Schutz Kritischer Infrastrukturen vor Computerangriffen auseinander setzt. Außerdem ist das im Mai 2004 geschaffenen Bundesamt für Bevölkerungsschutz und Katastrophenhilfe zu nennen, welche für den physikalischen Schutz Kritischer Infrastrukturen[60] zuständig ist. Darüber hinaus lassen sich verschiedene Zuständigkeiten beim Wirtschaftsministerium, dem Verteidigungsministerium oder den Nachrichtendiensten finden.

Die Problematik der Kritischen Infrastrukturen wird unter anderem durch die Unterschiedlichkeit der Bedrohungen und durch hohe Interdependenz der Strukturen untereinander erschwert. So können Ausfälle durch Naturkatastrophen hervorgerufen werden, aber auch durch menschliches Versagen sowie technische Fehler und Unfälle. Darüber hinaus ist das Feld der Akteure, die willentlich Kritische Infrastrukturen gefährden könnten sehr breit. Es reicht von Staaten, die militärisch Kritische Infrastrukturen angreifen könnten, über substaatliche Akteure (wie Terroristen) hin zu Einzeltätern (wie verärgerte Angestellte oder pubertierende Jugendliche). Die Interdependenz der Strukturen wird durch Rationalisierungen und Just-in-Time-Produktion noch problematischer, da schon kleine Ausfälle zu deutlichen Störungen führen können. Ersichtlich wurden die Abhängigkeiten in der Wirtschaft durch die Nachwirkungen des 11. Septembers. Da bestimmte Transporte nicht mehr reibungslos verliefen konnten einige Autofabriken nicht mehr weiter produzieren.[61]

Der Betrieb Kritischer Infrastrukturen wird heute maßgeblich durch Computertechnik beeinflusst, indem beispielsweise Produktionsanlagen mit Hilfe von Rechnersystemen gesteuert oder überwacht werden. Es besteht nun die Sorge, dass Angreifer die Vernetzung ausnutzen könnten, um mit Hilfe einfachster PC-Technologie wichtige Funktionen von Staaten zu stören. Praktische Beispiele lassen sich allerdings eher selten finden. Der einzige erfolgreiche Fall, in dem ein Mensch mit Absicht Kritische Infrastrukturen mit Hilfe von Computern angriff, ist in Australien bekannt geworden: Ein entlassener Angestellter der Stadtwerke einer Gemeinde wollte sich rächen und brach mit Hilfe seines Laptops über eine drahtlose Verbindung in das Wasserkontrollsystem seines ehemaligen Arbeitgebers ein. Er öffnete Schleusentore, woraufhin sich die Kloake in das örtliche Flusssystem ergoss. Menschen kamen nicht zu schaden, allerdings gab es starke ökologische Konsequenzen.[62] Neben diesem intendierten Angriff entstehen Störungen Kritischer Infrastrukturen als Nebeneffekt zu Internet-Vorfällen. So gelangte ein Computerwurm Anfang 2003 in das Kontrollnetzwerk eines Atomkraftwerkes und blockierte das digitale Kontrollsystem. Schaden konnte dadurch verhindert werden, dass es ein analoges Backup-System gab.[63] Der gleiche Wurmausbruch führte dazu, dass Tausende Geldautomaten einer US-amerikanischen Bank nicht mehr funktionierten.[64] Eine andere Bank wurde im Sommer 2003 durch einen anderen

---

59 Siehe http://www.bsi.bund.de/fachthem/kritis/index.htm (07.07.2005).

60 Siehe http://www.bva.bund.de/zivilschutz/kritis/index.html (07.07.2005).

61 Elhefnawy, Nader (2004): *Societal Complexity and Diminishing Returns in Security*, in: International Security, Jg. 29, Nr. 1, S. 152-174, S. 164.

62 Garrison, Linda / Grand, Martin (Redaktion) (2002): *National Infrastracture Protection Center – Highlights*, 2002(3) www.iwar.org.uk/infocon/ nipc-highlights/2002/highlight02-03.pdf (07.07.2005).

63 Busch, Christoph / Wolthusen, Stephen (2003): *Information Warfare: Threats to Critical Infrastructures*, in Proceedings of the XV International Amaldi Conference of Academies of Science and National Scientific Societies on Problems of Global Security, Helsinki, http://www.wolthusen.com/publications/Amaldi2003.pdf (07.07.2004); Poulsen, Kevin (2003): *Slammer worm crashed Ohio nuke plant network*, in: SecurityFocus 19. August 2003, http://www.securityfocus.com/news/6767 (07.07.2005).

64 Krebs, Brian (2003): *Internet Worm Hits Airline, Banks*, in: Washington Post 26. Januar 2003, http://www.washingtonpost.com/ac2/wp-dyn/A46928-2003Jan26 (05.06.2004).

Wurm betroffen, der wiederum zur Abschaltung von Geldautomaten führte. In Deutschland hatte ein Computerwurm im Frühjahr 2004 die Konsequenz, dass die Postbank nicht mehr ordnungsgemäß arbeiten konnte.[65]

Neben den ausgenutzten Verwundbarkeiten existieren diverse, teils theoretische Verwundbarkeiten, welche in Zukunft ausgenutzt werden könnten. Zum einen ist das „Überschwemmen" (Flooding) vom Computernetzwerken (wie dem Internet) mit Datenmüll zu nennen. Als Folgen sind neben einem durch Überschwemmung produzierten Ausfall von Geschäftsprozessen auch der Ausfall von Kommunikationsverbindungen von Infrastrukturen zu nennen.[66] Theoretisch wurde die Überschwemmung des Internets schon 2001 durch Weaver gezeigt.[67] Er konstruierte einen „Wurm", welcher innerhalb von 15 Minuten genug Rechner im Internet infizieren kann, die dann Datenmüll in alle Informationsleitungen senden, so dass eine normale Kommunikation nicht mehr möglich ist. Schon wenig später wurde ein weiteres Gedankenexperiment erstellt, mit dem gezeigt wurde, dass der Vorgang in wenigen Minuten erfolgen kann.[68] Der kurze Ausbreitungszeitraum führt dazu, dass keine Gegenmaßnahmen getroffen werden konnten, welche bei allen bis jetzt bekannten Würmern möglich waren. Eine zweite theoretische Verwundbarkeit besteht darin, dass das Internet, zumindest auf der logischen Ebene, inzwischen von einigen Knotenpunkten und Leitungen abhängig ist. Die Menge dieser bedeutenden Knoten wird mit ungefähr 10% bis 15% aller Knoten eingeschätzt. Würden diese Knoten zerstört werden, könnte es zu Teilung des Netzes in nicht verbundene Subnetze kommen.[69] Physikalisch ist das weltweite Netz wahrscheinlich von noch weniger Leitungen und Knotenpunkten abhängig. Im Auftrag eines Datendienstleisters konnte gezeigt werden, dass nur zwei Stellen im Netz zerstört werden müssen, um für ein Netz innerhalb der USA eine Trennung in Ost- und Westküste zu erreichen.[70]

Das tatsächliche Bedrohungspotential durch Terroristen ist heute umstritten. Ende der 1990er Jahre ist an der „Naval Postgraduate School" eine Studie[71] entstanden, die drei Entwicklungsstufen für erfolgreiche Angriffe auf Kritische Infrastrukturen mit Hilfe von Computern entwickelte. Nur eine Terrororganisation, die die dritte Stufe erreichen würde, hätte die Fähigkeit, effektiv mit Hilfe von Computern Kritische Infrastrukturen anzugreifen. Diese dritte Stufe ist dabei nur mit einem hohen Lern-, Organisations- und Ressourcenaufwand erreichbar. Die Autoren gingen davon aus, dass es fünf unterschiedliche Arten von Terrororganisationen gibt: Religiöse, ethno-nationalistische / separatistische, revolutionäre, rechtsextreme und „New Age"-Gruppen. Nur eine Art, der religiös motivierte Terrorismus, könnte nach Meinung der Autoren Interesse und die Fähigkeiten entwickeln, die dritte Stufe zu erreichen. Ein anschließender Workshop, bei dem ehemalige und aktive Mitglieder von Terrororganisationen anwesend waren, deutete darauf hin, dass Terrororganisationen sich der Möglichkeiten von Computerangriffen auf Kritische

---

65 Allerdings war nicht der Wurm direkt dafür verantwortlich. Vielmehr wurden, zum Schutz vor dem Wurm restriktivere Firewallregeln installiert, die eben auch den normalen Geschäftsverkehr der Bank behinderten.

66 Beispiele hierfür sind im Energiebereich zu finden. So werden immer mehr Komponenten der Energieversorgung mit Hilfe von Kommunikationsleitungen und Industrierechnern, so genannten SCADA-Systemen, ferngesteuert.

67 Weaver, Nicholas (2001): *Warhol Worms: The Potential for Very Fast Internet Plagues*, http://www.cs.berkeley.edu/~nweaver/warhol.htm (07.06.2004).

68 Staniford, Stuart / Grim, Gary / Jonkman, Roelof (2001): *Flash Worms: Thirty Seconds to Infect the Internet*, Silicon Defense, http://richie.idc.ul.ie/eoin/SILICON%20DEFENSE%20-%20Flash%20Worm%20Analysis.htm (12.05.2004).

69 Gorman, Sean P. / Schintler, Laurie / Kulkarni, Raj / Stough, Roger R. (2004): *The Revenge of Distance: Vulnerability Analysis of Critical Information Infrastructure,* in: Journal of Contingencies and Crisis Management, Jg. 12, Nr. 2, S. 48-63.

70 Ebd.

71 Nelson, Bill / Choi, Rodney / Iacobucci, Michael (1999): *Cyberterror Prospects and Implications*, White Paper, erschienen am Center for the Study of Terrorism and irregulare Warfare der Naval Postgradute School, http://www.nps.navy.mil/ctiw/files/Cyberterror%20Prospects%20and%20Implications.pdf (04.06.2004).

Infrastrukturen wenig bewusst sind.[72] Gleichwohl wurde argumentiert, dass eine neue Generation von Terroristen eher bereit und vor allem fähig wäre, Computer als Terrormittel einzusetzen, da für sie der Umgang mit der entsprechenden Technologie alltäglicher sei.[73]

Neben den eher theoretischen Überlegungen, ob Terroristen die Fähigkeit haben könnten, Anschläge auf Kritische Infrastrukturen durchzuführen, gab es in den letzten Jahren unterschiedliche staatliche Übungen. Diese sollten einen praktischen Überblick über die Verwundbarkeit Kritischer Infrastrukturen gegenüber Angreifern liefern. Dabei sind drei staatliche Übungen aus deutscher Sicht von größerem Interesse. Zum einen sind die US-amerikanischen Übungen „Eligible Receiver" (1997) und „Electronic Pearl Harbour" (2002) zu nennen, zum anderen das deutsche Planspiel „Cyber Terror Exercise" (CYTEX) (2001). In keinem Fall wurden sämtliche Ergebnisse und Protokolle der Übungen veröffentlicht. Vielmehr ranken sich Behauptungen um die Übungen, welche sich zum Teil widersprechen. „Eligible Receiver" war eine Übung des US-Verteidigungsministeriums, in der die Verwundbarkeit der Armee gegenüber Cyber-Angriffen getestet werden sollte. Im Zuge des Manövers konnten Angestellte der „National Security Agency" (NSA) angeblich mit Hilfe von normaler Software in Energiekontrollstellen eindringen. Sie hätten daraufhin den Strom in den USA abschalten können.[74] Dieses wurde als Beweis dafür genutzt, dass es für Terroristen relativ einfach sein könnte, mit Hilfe von Computern das Stromnetz der USA zu stören. Die Übung „Electronic Pearl Harbour" wurde von der „Gartner Group" und der „Naval Postgraduate School" mit dem Ziel durchgeführt, die Angreifbarkeit der Kritischen Infrastrukturen mit Hilfe des Telekommunikationsnetzes zu testen. Das Ergebnis scheint gewesen zu sein, dass ein (sowohl zeitlich wie auch räumlicher) Angriff nur sehr begrenzt wirksam sein könnte, einen hohen finanziellen Aufwand erfordern würde und eine lange Vorlaufphase benötige.[75] CYTEX als einzig bekannte deutsche Übung, wurde vom „Arbeitskreis Schutz von Infrastrukturen" (AKSIS)[76] veranstaltet und sollte die Reaktion der Behörden und großer Unternehmen auf Computerangriffe simulieren. Obwohl im Rahmen der Übung argumentiert wurde, dass das Szenario realistisch sei[77], wurde der Erfolg eines Angriffes vorausgesetzt.[78] Die Übung erlaubt deswegen wenig Rückschlüsse auf die Möglichkeit terroristischer Angriffe auf Kritische Infrastrukturen.

Obwohl die Diskussion um die Verwundbarkeit von Kritischen Infrastrukturen als allgemein etabliert gelten kann und es bereits in der Vergangenheit zu Störungen durch Naturereignisse oder menschliches Versagen gekommen ist, sind (bis auf die australische Ausnahme) noch keine von Menschen absichtlich herbeigeführten Störungen bekannt geworden. Dennoch erfolgt eine praktische Beschäftigung mit dem Schutz Kritischer Infrastrukturen, auch vor gezielten Angriffen. Hierbei ist zwischen unterschiedlichen Sichtweisen und damit verschiedenen Umgänge zu unterscheiden:

1. Die Sicht aus der Perspektive der IT-Sicherheit. Hierbei wird versucht, die einzelnen Computersysteme technisch zu schützen.
2. Die betriebswirtschaftliche Sicht. Hierbei werden neben den technischen Gesichtspunkten auch organisatorische und andere Aspekte berücksichtigt.

---

72 Tucker, David (2000a): *The Future of Armed Resistance: Cyberterror? Mass Destruction?*, http://www.nps.navy.mil/ctiw/files/substate_conflict_dynamics.pdf (03.06.2004).

73 Nelson et al., Cyberterror.

74 Gertz, Bill (1998): *Computer hackers could disable military*, in: The Washington Times, 16. April 1998, http://www.newdimensions.net/headlines/m02.htm (07.05.2004).

75 Wilson, Clay (2003): *Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress*, CRS Report to Congress RL 32114, http://www.fas.org/irp/crs/RL32114.pdf (04.06.2004)

76 Siehe http://www.aksis.de/ für mehr Informationen.

77 Hutter, Reinhard (2002): *Cyber Terror – eine realistische Gefahr*, in: Das Parlament 8. März 2002, http://www.aksis.de/Hutter-Cyber-Terror.pdf (04.06.2004).

78 Hess, Sigurd (2003): Informationssicherheit und Schutz kritischer Infrastrukturen, URL: http://www.dmkn.de/1779/technologie.nsf/D9F02C2A100B89D7C1256CD80037695B/$File/itsicherheit.pdf (03.06.2004)

3. Die Sicht der Strafverfolgungsbehörden und
4. Die Sicht unter Gesichtspunkten internationaler Sicherheit, wobei der letzte Blickwinkel sicher der umfassendste und komplexeste ist.[79]

In den USA findet zumindest in Fachkreisen eine Auseinandersetzung mit dem Schutz Kritischer Infrastrukturen vor Computerangriffen statt. Als Beispiel ist die „National Strategy to Secure Cyberspace (NSSC)“[80] zu nennen, welche 2003 veröffentlicht wurde. Zuvor durchlief die NSSC eine Diskussionsphase, die durch zehn „Town Hall Meetings“ gekennzeichnet war. Diese Meetings sollten die Meinungen der Industrie und von Privatpersonen in den Entwurf der Strategie einbeziehen, um einen weitreichenden Kompromiss zu erreichen. In Deutschland hat es bis jetzt noch keine öffentliche Auseinandersetzung mit dem Thema gegeben. Auch sind keine Initiativen seitens der Legislative zu erkennen, Kritische Infrastrukturen zu schützen. Seitens der Exekutive scheint es zwar unterschiedliche Studien zu geben (z. B. beim BSI), die aber nicht veröffentlicht sind. Allerdings wird von Seiten des BSI zugegeben: „The German system for the protection of critical infrastructures is not very transparent to outsiders.”[81] Aufgrund dieser Intransparenz ist es unwahrscheinlich, dass es zu einer offenen Diskussion ähnlich zu den USA wird, kommen wird.

Weiterführende Forschungsfragen

- Können aus Datennetzen Angriffsmuster ausgefiltert werden?
- Wie groß sind Redundanzen in den Infrastrukturen?
- Welchen Einfluss haben deutsche Datenschutzbestimmungen auf Schutzstrategien?
- Wie ist das Potential bekannter Terrororganisationen in Bezug auf Computerangriffe einzuschätzen?
- Ist ein wirksamer Schutz mittels der zugrunde liegenden Technologie überhaupt möglich?
- Muss zum Schutz Kritischer Infrastrukturen tatsächlich in Bürgerrechte eingegriffen werden?

2. Reaktionen der Gesetzgeber

Nachdem ein exemplarischer Überblick über drei mögliche Gefährdungsbereiche gegeben wurde, soll in diesem Kapitel deutlich gemacht werden, welche Aktionen vom Gesetzgeber und der Exekutive ergriffen wurden, um effektiver als bisher auf Terroranschläge reagieren zu können. Dabei wird das Augenmerk heute zunächst nicht so stark auf die Prävention gelegt, sondern eher auf die direkte Verhinderung von Anschlägen bzw. die Nachsorge nach erfolgten Anschlägen.

A) Das Terrorismusbekämpfungsgesetz

Als Reaktion auf die Terroranschläge vom 11. September 2001 verabschiedete der Bundestag zwei „Sicherheitspakete“, zur Terrorismusbekämpfung. Das zweite Paket ist durch das „Gesetz zur Bekämpfung des Internationalen Terrorismus“, kurz

[79] Dunn, Myriam (2004): *Sicherheit im Informationszeitalter*, in: digma 2004(2), http://www.isn.ethz.ch/crn/_docs/sicherheit_im_infozeitalter.focus.pdf
[80] White House (2003): *The National Strategy to Secure Cyberspace*, www.securecyberspace.gov/ (07.07.2005).
[81] Ritter / Weber, Critical Infrastructure Protection.

Terrorismusbekämpfungsgesetz, in Kraft getreten. Das Gesetz selber beschreibt ausschließlich Erweiterungen der Befugnisse von Geheimdiensten und Polizei. Der Zweck ist die bessere Überwachung und Verfolgung von Individuen, welche in den internationalen Terrorismus verstrickt sein könnten. . Außerdem soll durch Gesetzesänderungen verhindert werden, dass „verdächtige" Personen in sicherheitsrelevanten oder lebenswichtigen Einrichtungen[82] arbeiten dürfen. Damit kann des Gesetz in die Kategorie der Gefahrenabwehr eingeordnet werden, weniger aber in die Kategorie der Nachsorge bei Terroranschlägen.

Das Gesetz wird aufgrund seiner tiefen Einschnitte in die Persönlichkeitsrechte kritisiert. Allerdings konnte auf das beschlossene Gesetz schon in der Beratungsphase Einfluss durch den Datenschutzbeauftragten genommen werden. Der 19. Tätigkeitsbericht[83] des Beauftragten zeigt welche Verbesserungen vorgenommen wurden, dass es aber auch immer noch datenschutzrechtlich bedenkliche Abschnitte gibt.[84] Nichts desto trotz schreibt der Datenschutzbeauftragte, dass das Gesetz ein guter Kompromiss zwischen „Sicherheit" und Datenschutz darstellen würde.

B) Das Luftsicherheitsgesetz

Das veränderte Luftsicherheitsgesetz[85] (verabschiedet im Bundestag am 16. Juni 2004) soll Terroranschläge „in letzter Sekunde" verhindern, indem es der Bundeswehr unter bestimmten Bedingungen erlaubt, Flugzeuge abzudrängen oder gar abzuschießen. Das Gesetz ist dabei als eine Reaktion auf die Terroranschläge des 11. September 2001 und auf das Kreisen eines Sportflugzeuges über Frankfurt am Main im Januar 2003. Das Gesetz wird noch immer von einer Diskussion über dessen Verfassungskonformität begleitet. Außerdem werden gegen das Gesetz ethische Argumente angeführt. Bei Überlegungen zur Verfassungsmäßigkeit wird damit argumentiert, dass es sich um einen Einsatz der Bundeswehr im Inneren handeln würde, der nur unter bestimmten Gesichtspunkten erlaubt ist. Weiterhin wäre es ein Eingriff des Verteidigungsministers in die innere Sicherheit, da er entscheiden darf, ob ein Flugzeug abgeschossen werden darf.[86] Darüber hinaus geht es um die Frage, ob durch einen Abschuss in das Grundrecht auf Leben eingegriffen würde.[87] Der letzte Punkt wird auch in ethischer Hinsicht diskutiert: Kann und darf man Menschenleben gegeneinander aufwiegen?[88] Ist es bspw. rechtens, ein Passagierflugzeug mit einer bekannten Zahl von Passagieren abzuschießen, um Schaden von einer u.U. unbekannten Zahl anderer Menschen abzuwenden?

Nach über einem halbem Jahr wurde das Luftsicherheitsgesetz von Bundespräsidenten Horst Köhler am 12. Januar 2005 unterzeichnet. Allerdings machte Köhler deutlich, dass er erhebliche Bedenken gerade im Bezug auf den Abschuss von Passagiermaschinen habe und deswegen zwecks rechtlicher Klärung das Bundesverfassungsgericht angerufen werden

---

82 Bspw. solche Einrichtungen, die für das Funktionieren des Gemeinwesens unabdingbar sind (Artikel 5 Terrorismusbekämpfungsgesetz).

83 Bundesbeauftragter für Datenschutz (2003): *Tätigkeitsbericht 2001 – 2002 des Bundesbeauftragten für de n Datenschutz - 19. Tätigkeitsbericht*, www.bfd.bund.de/information/19tb0102.pdf (07.07.2005).

84 Onlinezugriff auf das Ausländerzentralregister durch Nachrichtendienste oder das Sammeln von Fingerabdruckdaten von Asylbewerbern.

85 Für den Entwurf der Regierung siehe http://dip.bundestag.de/btd/15/023/1502361.pdf, bzw. die Beschlussempfehlung und den Bericht in der Bundestagsdrucksache 15/3338 (http://dip.bundestag.de/btd/15/033/1503338.pdf) sowie die Debatten im Bundestag: 15/89 (http://dip.bundestag.de/btp/15/15089.pdf), 15/115 (http://dip.bundestag.de/btp/15/15115.pdf) (alle 07.07.2005).

86 Soria, José Martínez (2004): *Polizeiliche Verwendungen der Streitkräfte*, in: Deutsches Verwaltungsblatt, Heft 10/2004, S. 597 – 605.

87 Baumann, Karsten (2004): *Das Grundrecht auf Leben unter Quantifizierungsvorbehalt? – Zur Terrorismusbekämpfung durch „finalen Rettungsabschuss"*, in: Die Öffentliche Verwaltung (DÖV) 2004, S. 853–861; Merkel, Reinhard (2004): *Wenn der Staat Unschuldige opfert*, in: Die Zeit, 2004(29).

88 Siehe Max Stadler (FDP) unter http://www.max-stadler.de/meldung.php?id=5816&tag=Positionen&BackURL=/freierubrik1.php (07.07.2005).

sollte.. Die Position der Regierung wurde von Bundesinnenminister Otto Schily während einer Bundespressekonferenz am 12. Januar 2005 noch einmal deutlich. Dabei argumentierte er, dass die Passagiere im Flugzeug, bei einer solchen Entscheidung, praktisch schon tot seien und es durch den Abschuss möglich wäre, andere Menschenleben zu retten. Ende Januar kündigten FDP-Politiker an, dass sie zusammen mit Verkehrs- und Privat-Piloten beim Verfassungsgericht Beschwerde gegen das Gesetz einlegen werden. Zuvor hatte Innenminister Schily im Bundestag angekündigt, dass man unter Umständen Änderungen am Gesetz vornehmen würde, um eine Beschwerde abzuwenden. Gleichzeitig wurde von der Regierungskoalition eine Grundgesetzänderung abgelehnt, da dadurch die Einsatzmöglichkeit der Bundeswehr im Inneren auf eine Art ausgedehnt würde, die nicht erwünscht sei.[89]

Analog zum Luftsicherheitsgesetz sind die Stimmen für eine Art „Seesicherheitsgesetz“ im letzten Jahr lauter geworden.[90] Ähnlich wie bei entführten Flugzeugen wird argumentiert, dass die Deutsche Marine keine Handhabe gegenüber Terroristen habe, die bspw. eine Fähre entführt hätten.[91] Unter anderem aus diesem Grund müsste die Marine in einer „Gesamtschau maritimer Sicherheitsinstrumente“ ein ähnlich „klärendes“ Gesetz wie das Luftsicherheitsgesetz erhalten.[92] Letztendlich geht es bei beiden Bereichen um die Diskussion, ob die Bundeswehr über die sehr stringente aktuelle Handhabe hinaus für Polizeiaufgaben im Sinne der „Inneren Sicherheit“ im Landesinneren eingesetzt werden dürfe, wie es die CDU/CSU fordert.[93]

C) Hafensicherheitsgesetz

Es besteht eine enge Verbindung des Luft- bzw. Seesicherheitsgesetz mit dem Hafensicherheitsgesetz. Den drei Gesetzen geht es hauptsächlich um die Verhinderung von Terroranschlägen, indem im voraus verstärkte Präventions- und Schutzarbeit, unter anderem durch die Polizei, ermöglicht wird. Ein Beispiel für ein Hafensicherheitsgesetz ist der Entwurf, welcher vom Senat der Freien und Hansestadt Hamburg[94] im Dezember 2004 verabschiedet wurde. Ähnlich wie bei dem Luftsicherheitsgesetz soll das Hafensicherheitsgesetz die Gefahr, die durch Anschläge auf Häfen entstehen könnte, mindern. Das Gesetz erfüllt dabei internationale Übereinkommen zum Schutz des menschlichen Lebens auf See (SOLAS[95]) und den Internationalen Kodex für die Gefahrenabwehr auf Schiffen und in Hafenanlagen (ISPS-Code[96]). Im Gesetz selber werden unter anderem Polizeiaufgaben im Zusammenhang mit dem Hafen genauer beschrieben, sowie die Zugangsmöglichkeiten von Risikobewertern und die Sicherheitsüberprüfung von Hafenmitarbeitern. Das Gesetz greift in das Grundrecht der Freiheit der Person ein und in das Grundrecht der Unverletzlichkeit der

89 *Klage gegen Abschuss-Gesetz*, in: die tageszeitung, 29./30.01.2005.

90 Siehe Interview mit Lutz Feldt (Marine Inspekteur) im Hamburger Abendblatt vom 11. Dezember 2004; Rede von Rainer Arnold (MdB, Verteidigungspolitischer Sprecher der SPD) auf der Marine Kommandeurstagung am 16. November 2004, http://www.spdfraktion.de/rs_datei/0,,4311,00.pdf (07.07.2005).

91 Härpfer, Susanne (2004): *Kein Schutz bei Terrorangriffen vor der Küste? Vom Luftsicherheitsgesetz zum Seesicherheitsgesetz, in Streitkräfte und Strategien* - NDR Info 7. Februar 2004 http://www.bits.de/public/ndrinfo/sunds070204.htm (07.07.2005).

92 Papenroth, Thomas (2004): *Die Zukunft der Deutschen Marine. Herausforderungen für die maritime Komponente der Bundeswehr*, SWP-Studie 2004/S 17, http://www.swp-berlin.org/produkte/swp_studie.php?id=3308&PHPSESSID=376aa2659ebfeca0457503961e8cc8b5 (08.07.2005).

93 Siehe hier z.B. den Gesetzentwurf der CDU/CSU Fraktion zur Änderung der Paragraphen 35 und 87a des Grundgesetzes (Bundestagsdrucksache 15/2649 http://dip.bundestag.de/btd/15/026/1502649.pdf (07.07.2005); Interview mit Dr. Wolfgang Schäuble im Deutschlandfunk am 11. März 2004, http://www.wolfgang-schaeuble.de/040311dlf.pdf (07.07.2005).

94 Siehe http://fhh.hamburg.de/stadt/Aktuell/pressemeldungen/2004/dezember/15/2004-12-15-hafensicherheit-gesetz,property=source.pdf (07.07.2005).

95 Für die Konvention, siehe http://www.imo.org/Conventions/contents.asp?topic_id=257&doc_id=647 (07.07.2005).

96 Als Einstiegspunkt: http://www.imo.org/Newsroom/mainframe.asp?topic_id=897 (07.07.2005).

Wohnung (Art. 13 GG). Die Problematik des Gesetzes besteht in der versuchten Erhöhung des Schutzniveaus mittels Eingriff in die Recht des Einzelnen, während jedoch genügend andere leicht zu findende Lücken vorhanden sind, durch die ein Unbefugter beispielsweise. auf ein Hafengelände gelangen kann. Es bleibt die Frage ob die Einschränkung der Bürgerrechte durch den nur minimalen Schutzzuwachs gerechtfertigt ist.

D) Neuorganisation des Bevölkerungsschutz

Während des Kalten eges sollte die Bevölkerung durch den Zivilschutz auf den Verteidigungsfall vorbereitet werden. Da dieser für wahrscheinlich gehalten wurde, entstand in Deutschland das effektivste Zivilschutzsystem in Europa (Geier 2002). Nach dem Fall der Mauer sank die Wahrscheinlichkeit, dass sich die Bevölkerung gegen den Angriff einer anderen Armee schützen müsste, wodurch die Zuteilung von Ressourcen für den Zivilschutz drastisch abnahm. Dieses änderte sich nach den verschiedenen Großkatastrophen der letzten Jahre, wie dem Oder- (1997) oder dem Elbehochwasser (2002). Um die Katastrophenhilfe der Bundesländer[97] zu verbessern und zu koordinieren, schuf die Bundesregierung 2004 unter Zustimmung der CDU/CSU und Ablehnung der FDP das neue Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK).[98] Hierbei wurde der Begriff Zivilschutz durch Bevölkerungsschutz ausgewechselt, um deutlich zu machen, dass sich die Vorbereitungen nicht mehr ausschließlich auf den Verteidigungsfall konzentrierten, sondern sehr viel breiter angelegt sind.

Das BBK hat folgende Aufgaben:[99]

- „Erfüllung der Aufgaben des Bundes im Bevölkerungsschutz (insbesondere ergänzender Katastrophenschutz, Maßnahmen zum Schutz der Gesundheit, Schutz von Kulturgut, Trinkwassernotversorgung),
- Planung und Vorbereitung von Maßnahmen im Bereich der Notfallvorsorge/Notfallplanung,
- Planung und Vorbereitung der Zusammenarbeit von Bund und Ländern bei besonderen Gefahrenlagen (Koordination des Krisenmanagements),
- planerische/konzeptionelle Vorsorge zum Schutz kritischer Infrastrukturen,
- Ausbildung, Fortbildung und Training im Bereich des Bevölkerungsschutzes und der Katastrophenhilfe,
- Katastrophenmedizin,
- Warnung und Information der Bevölkerung,
- Ausbau der Katastrophenschutzforschung, insbesondere im ABC-Bereich,
- Stärkung der bürgerschaftlichen Selbsthilfe,
- Konzeptionell-planerische Aufgaben im Bereich der internationalen Zusammenarbeit unter Beteiligung aller nationalen Stellen des Zivilschutzes.“

Hervorgegangen ist das BBK aus der Zentralstelle Zivilschutz des Bundesverwaltungsamtes. Nach Meinung der CDU/CSU besteht durch diese Umwidmung die Gefahr, dass es sich nur um eine Änderung des Namensschildes und nicht um einen ernsthaften Versuch der

[97] Die Katastrophenhilfe ist in Deutschland Ländersache, während der Zivil- oder Bevölkerungsschutz auf Bundesebene organisiert ist.
[98] Für mehr Informationen, siehe http://www.zivilschutz-online.de (07.07.2005).
[99] Aus Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK): http://194.95.178.54/zivilschutz/zfz/index.html (07.07.2005).

Regierung handele, dem Bevölkerungsschutz einem höheren Stellenwert zuzuschreiben.[100] 2004 betrug das Budget des Amtes 84 Mio. Euro (10 Mio. mehr als das Budget für die ehemalige Abteilung beim Bundesverwaltungsamt) und ist in Bonn angesiedelt.

Neben der „Namensschildproblematik" wird von der FDP kritisiert, dass das Bundesamt selber nicht genug Kompetenzen habe, sondern vielmehr ein Planungsstab sei. Darüber hinaus brauche man das neue Amt nicht, da die alten Strukturen ausreichten und durch ein neues Amt letztendlich nur verkompliziert würden „Ich habe noch kein einziges Mal erlebt, dass mit einem neuen Amt irgendetwas besser geworden wäre in Deutschland (Gisela Piltz)."[101] Trotz der genannten Kritik wird das Ziel, welches mit dem Bundesamt verfolgt wird, von allen Parteien befürwortet.

Zum BBK gehört die Akademie für Krisenmanagement, Notfallplanung und Zivilschutz (AKNZ)[102], die bei der Ausbildung von Katastrophenhelfern beteiligt ist und gleichzeitig den Bevölkerungsschutz in Deutschland wissenschaftlich begleitet.

E) Warnung der Bevölkerung

Zur Zeit des Kalten Kriegs konnte die Bevölkerung über ein weit ausgedehntes Netz von Sirenen sehr schnell gewarnt werden. Das Netz umfasste ca. 65.000 Sirenen, welche über Standleitungen angesteuert werden konnten. Nach Ende des Kalten Krieges wurde das Sirenennetz 1992 aufgegeben, wodurch die Möglichkeit verloren ging, die Bevölkerung schnell zu warnen. Ein Großteil der Sirenen (ca. 35.000 – 40.000) ist allerdings an die Städte und Gemeinden übergegangen, die sie zur Brandwarnung und zum Katastrophenschutz nutzen können. Zur Warnung der Bevölkerung besteht auf Bundesebene ein Satellitensystem, welches es den Behörden ermöglicht, Warnmeldungen an Radio und Fernsehstationen zu senden. Diese sind verpflichtet, die Warnung sofort an die Hörer bzw. Zuschauer weiter zu geben.[103]

Der große Nachteil des Systems ist, dass die Bevölkerung nur gewarnt werden kann, wenn sie das Radio oder den Fernseher eingeschaltet hat, was zumindest nachts eher nicht der Fall sein dürfte. Aus diesem Grund wird seit einigen Jahren ein System entwickelt, welches die Vorteile des alte Sirenensystems mittels neuer Technologie wieder herstellt. Dabei wird sowohl an Mobilfunknachrichten gedacht, als auch an die Nutzung von Funkuhren, speziell präparierten Radios oder die Nutzung des normalen Telefonnetzes. Allerdings befindet sich ein solches System noch in der Planung und es ist zu erwarten, dass die Verfügbarkeit noch einige Zeit auf sich warten lassen wird.[104]

Bewertung

Nach Ende des Kalten Krieges wurden, als eine Art Friedensdividende, die Kosten für den Zivilschutz eingespart und Kapazitäten abgebaut. Heute steht man jedoch wieder vor einer ähnlichen Situation: Der Staat muss für große Katastrophen, seien sie von der Natur oder von Menschen hervorgerufen, vorsorgen und die alten Strukturen wieder aufbauen. Die Arbeiten in diesem Bereich scheinen zwar anzulaufen, allerdings nur mit sehr geringer Intensität – wie unter anderem beim Bereich „Warnung der Bevölkerung" ersichtlich wird. Darüber hinaus zeigen sich grundsätzlich unterschiedliche Sichtweisen in der Beurteilung von Mitteln, im

[100] Siehe hierzu die Äußerungen von Frau Philipp zur 2. und 3. Lesung des Gesetzes über die Errichtung des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe (Plenarprotokoll 15/94).
[101] Geäußert in der 94. Sitzung des 15. Bundestages (4. März 2004).
[102] Vgl. http://194.95.178.54/zivilschutz/aus_und_weiterbildung/index.html (07.07.2005).
[103] Schulz, Jürgen (2003): *Warnsysteme in Gegenwart und Zukunft*, in: Notfallvorsorge 2003(3), S. 5-7.
[104] Ebd.

besonderen über den Einsatz der Bundeswehr. Das schleppende Vorankommen in vielen Bereichen lässt sich wahrscheinlich mit der fehlenden akuten Bedrohung und den Haushaltssparzwängen erklären. Hier sollte die Politik schneller arbeiten, da die letzten Jahre gezeigt haben, dass sich Naturereignissen mit katastrophalen Auswirkungen häufen. Erfolgt eine Vorbereitung auf Naturkatastrophen, werden gleichfalls, praktisch nebenbei, Kapazitäten zur Reaktion auf terroristische Angriffe aufgebaut.

Weiterführende Forschungsfragen

- Warum gibt es nur sehr wenig gesetzliche Initiativen im Bereich der Nachsorge bei Terroranschlägen?
- Hat es durch Schaffung des BBK substanzielle Verbesserungen im Bevölkerungsschutz und der Katastrophenhilfe gegeben oder war die Schaffung nur eine „Türschildänderung“?
- Wie lassen sich die Auswirkungen des Terrorismusabwehrgesetzes bewerten?
- Rechtfertigt der Erfolg der präventiven Terrorismusabwehrmaßnahmen die Einschränkung der bürgerlichen Freiheiten, wie beispielsweise die Einschränkung des Fernmeldegeheimnisses?

3. Die wissenschaftliche und gesellschaftliche Debatte

Obwohl schon länger in der Diskussion, gewannen zwei unterschiedliche Punkte in der Debatte um Kriminalität und Terrorismus nach dem 11. September 2001 an Bedeutung:

1. Der Einsatz der Bundeswehr im Inneren,
2. Die Aufhebung des Trennungsgebotes[105] zwischen Geheimdiensten und Polizei.

Sowohl das heute nur noch eingeschränkte Verbot des Einsatzes der Bundeswehr im Inneren als auch das Trennungsgebot stammen aus den Erfahrungen des Dritten Reiches.[106] Diese historischen Erfahrungen werden von einigen Autoren als antiquiert und nachteilig für die Verhinderung von Terroranschlägen gesehen. So argumentiert Eckard Wertbach, ehemaliger Präsident des Bundesamtes für Verfassungsschutz und ehemaliger Berliner Innensenator, dass die Strafverfolgungsbemühungen und die Arbeit der Geheimdienste zu zersplittert seien. Deswegen fordert er eine gemeinsame Datenbank, auf die sowohl die Landeskriminalämter und das BKA als auch die Geheimdienste zugreifen können.[107] Durch einen gemeinsamen Zugriff würde allerdings das Trennungsgebot unterlaufen werden. Ähnlich argumentiert Thamm[108], der meint, dass das Trennungsgebot faktisch schon aufgehoben sei, da es beispielsweise im Bereich der Menschenschleusung ein „Informations-Board“ unter Einbezug

[105] „Dieses Trennungsgebot ist in Abgrenzung gegen die Verschmelzung von nachrichtendienstlichen und polizeilichen Befugnissen in der Praxis der Gestapo und des "Reichssicherheitshauptamtes" des NS-Regimes entwickelt worden. Seine Grundlage ist das Rechtsstaatsprinzip des Grundgesetzes: Institutionen, die mit nachrichtendienstlichen Mitteln der Aufklärung und des Beobachtens im Vorfeld von Gefahren dienen, sollen strikt getrennt werden von polizeilichen Institutionen, die mit Eingriffs- und Zwangsbefugnissen ausgestattet sind und deren Befugnisse auf Gefahrenabwehr und Strafverfolgung begrenzt sind.“ Seifert, Jürgen (1997): *Geheimdienste und Polizei: Trennung als Machtbeschränkung*, in: Humanistische Union (Hrsg.) (1997): *Grundrechtsreport 1997*, http://report.humanistische-union.de/1997/grundrechte_report1997/37.htm (07.07.2005).

[106] Während des Dritten Reiches wurde die Wehrmacht gegen die eigenen Bevölkerung eingesetzt. Durch Artikel 35 Grundgesetz wird ein Einsatz der Bundeswehr im Inneren nur unter eng begrenzten Ausnahmen erlaubt

[107] Werthebach, Eckart (2004): *Deutschland: auf den Terror schlecht vorbereitet*, In Internationale Politik, Jg. 59, Nr. 2, S. 29-33.

[108] Thamm, Berndt Georg (2003): *Ist das Trennungsgebot noch aktuell?*, in: Hirschmann, Kai / Leggemann, Christian (Hrsg.) (2003): *Der Kampf gegen den Terrorismus: Strategien und Handlungserfordernisse in Deutschland*, Berliner Wissenschafts-Verlag, S. 235-254.

des BKA, des BND und anderer Dienste gäbe. Thamm kommt deswegen zu dem Schluss, dass die deutsche Fragestellung nach der Aktualität des Trennungsgebotes eindeutig negativ beantwortet werden müsste.[109]

Der Einsatz der Bundeswehr im Inneren ist für einige Autoren in verschiedenen Lagen denkbar. So wird davon ausgegangen, dass die Bundeswehr Objektschutzaufgaben wahrnehmen könnte. Außerdem verfüge nur sie über Abstandswaffen, um Angriffe durch Schiffe abzuwehren.[110] Darüber hinaus werden die Streitkräfte schon heute im Inneren eingesetzt, sei es durch Kampfflugzeuge, die mit Wärmebildkameras ausgestattet sind und so Entführungsopfer in Waldgebieten aufspüren sollen[111] oder bei Großkatastrophen wie der Oderflut 2002.

Darüber hinaus wird diskutiert, ob die Trennung zwischen Bundes- und Landesebene beim Verfassungsschutz noch angemessen ist. So sei die Konstruktion einzigartig in der Welt und würde Barrieren für den Informationsaustausch darstellen. Darüber hinaus würde eine Zusammenlegung zu Synergieeffekten führen. Außerdem könnte es sein, dass die gegenwärtige Trennung zu einer Überlastung auf Landesebene führen würde, da der Verfassungsschutz auf Landesebene sich schon um Rechtsextremismus, die Fundamentalistenszene und um Spionageabwehr kümmern müsse.[112] In eine ähnliche Richtung argumentiert der BKA-Präsident Jörg Ziercke in Bezug auf polizeiliche Prävention von Terrorismus. Er fordert, dass das Verbot der präventiven Gefahrenabwehr, welches für das BKA gelte, und die Aufgabentrennung zwischen LKAs und BKA beides aufzuweichen sei. So sollte das BKA alleine für die Terrorismusabwehr zuständig sein, das es der Organisation leichter sei, über die Bundesländergrenzen hinweg zu handeln.[113]

Ähnlich scheint die Lage beim Katastrophenschutz zu sein. In Deutschland hat die Freiwillige Feuerwehr 1,2 Millionen Mitglieder. Darüber hinaus sind 0,5 Mio. freiwillige Helfer in den fünf Hilfsorganisationen Deutsches Rotes Kreuz, Arbeiter-Samariter Bund, Deutsche Lebensrettungsgesellschaft, Malteser Hilfsdienst und Johanniter Unfall-Hilfe organisiert. Außerdem kann das Technische Hilfswerk auf 50.000 Freiwillige zurückgreifen. Angesichts dieser Organisationszahlen sollte Deutschland weltweit führend beim Bevölkerungsschutz sein. Gleichwohl wird argumentiert, dass die Aufgabentrennung zwischen Bund und Ländern zu erheblichen Reibungen führe, welche den Katastrophenschutz ineffektiver mache, als er sein könnte.[114] Allerdings gibt es seit der Oder-Flut 1997, spätestens aber seit 2002 neuere Entwicklungen, die zu einer stärkeren Zusammenarbeit zwischen Bund und Ländern und zu einer gewissen Zentralisierung von Ressourcen führen sollen. Der Erfolg der Veränderungen wird aber unterschiedlich beurteilt.[115]

Weiterhin wird kritisiert, dass die Polizei zu schlecht ausgerüstet sei, um sinnvolle Terrorprävention betreiben zu können. Dabei wird sich sowohl auf die personelle Ausstattung bezogen als auch auf die materielle. So seien in den letzten Jahren immer noch Stellen bei der Polizei gestrichen worden. Darüber hinaus liege die Ausstattung im Vergleich zu den europäischen Nachbarn zurück. Die deutsche Polizei funkt immer noch analog, und ist damit, neben Albanien, das einzige Land, dass nicht auf abhörsichere Übertragungstechnik setzen

---

109 Thamm, Ist das Trennungsgebot noch aktuell?, S. 247.

110 Werthebach, Deutschland: auf den Terror schlecht vorbereitet.

111 Leggemann, Christian (2003): *Der Einsatz von Streitkräften zur Terrorismusbekämpfung - Die aktuelle Debatte in Deutschland*, in: Hirschmann, Kai / Leggemann, Christian (Hrsg.) (2003): *Der Kampf gegen den Terrorismus: Strategien und Handlungserfordernisse in Deutschland*, Berliner Wissenschafts-Verlag

112 Bauer, Michael (2002): *Terrorismus - Bedrohungsszenarien und Abwehrstrategien*, München, Hanns-Seidel-Stiftung e.V., http://www.extremismus.com/texte/isex6.pdf (07.07.2005).

113 „*Jeder Dorfpolizist darf das*“, die tageszeitung, 7. Februar 2005, S. 4.

114 Meyer-Teschendorf, Klaus-G. (2003): *Neue Strategie für die zivile Sicherheitsvorsorge*, in: Notfallvorsorge, 2003(2), S. 5-8.

115 Rosen, Klaus-Henning (2004): *Zurück ins 19. Jahrhundert? Ungereimtheiten der Länderstrategien im Katastrophenschutz*, in: Notfallvorsorge 2004(2), S. 5-7; Liebländer, Benedikt (2004): *Ungereimtheiten der Länderstrategie im Katastrophenschutz oder intelligente Lösung?*, in: Notfallvorsorge 2004(3), S. 5-6.

kann, die sich auch zur Übermittlung von Daten[116] eignen würde.[117]

Im ZDF wurde im Dezember 2004 eine Sendung unter dem Titel „Tag X: Wie gut ist Deutschland vorbereitet“[118] ausgestrahlt. In der Sendung wurden das Szenario eines Terroranschlag und seiner Folgen simuliert, um den Zuschauern den Stand der deutschen Vorbereitungen darzulegen. In anschließenden Expertendiskussionen wurde argumentiert, dass auf der einen Seite schon bestimmte Vorbereitungen getroffen sein, auf der anderen Seite der Katastrophenschutz aber immer noch nicht genug ausgearbeitet sei und sowohl bei den Katastrophenhelfern, als auch bei den Strafverfolgungsbehörden (Nachrichtendienste und Polizei) immer noch nicht genug Personal und Ressourcen vorhanden seien. In einer Abstimmung auf der Webseite wird deutlich, dass ein Großteil der an der Befragung Teilnehmenden glaubt, dass Deutschland nicht gut vorbereitet sei (77%).[119] Allerdings wird auf der Seite nicht ersichtlich, wie lange die Abstimmung durchgeführt wurde. Zur Zeit scheinen aber keine neuen Stimmen entgegen genommen zu werden.

Im Kapitel 1.a wurde im „vierten Weg“ der Angriff von Terroristen auf Kernkraftwerke genannt. Hierzu gibt es in der öffentlichen Diskussion zwei unterschiedliche Schutzvorstellungen. Auf der einen Seite wird erwogen, die Kraftwerke bei Annäherung eines Flugzeuges einzunebeln, auf der anderen Seite sollen große Betonpfeiler im Umkreis um die Kraftwerke aufgestellt werden, die den Einschlag eines Flugzeuges in die Nuklearanlage verhindern sollen. Eine dritte Option wird nicht in Betracht gezogen: Sowohl in Frankreich als auch in Tschechien werden Flugabwehrraketen für Krisensituationen um Kraftwerke stationiert. Aufgrund der engen Bebauung ist dieses in Deutschland aber nicht praktikabel.

Das Einnebeln von Kernkraftwerken gilt als kostengünstige Lösung, die relativ schnell realisiert werden kann. Dazu werden in einem bestimmten Umkreis um das zu schützende Kraftwerk Nebelwerfer installiert.[120] Nähert sich ein Flugzeug dem Kraftwerk bis auf 15 Kilometer ,werden Nebelgranaten abgeschossen, die das Kraftwerk umhüllen sollen. Im besten Fall kann der „angreifende“ Pilot das KKW nicht mehr sehen und wendet das Flugzeug ab. Allerdings gibt es unterschiedliche Probleme bei der (schon vorgeführten) Methode. So sind manche Flugstraßen nicht 15, sondern nur zwei Kilometer von einem KKW entfernt. Es bleibt deswegen nicht genügend Vorwarnzeit. Des weiteren funktioniert die Einnebelung nur bei bestimmten Wetterbedingungen. Weht zum fraglichen Zeitpunkt starker Wind, kann sich der Nebel nicht lange genug halten. Darüber hinaus ermöglichen es aktuelle Navigationssysteme auch ohne Sicht einen bestimmten Punkt anzusteuern. Selbst wenn das im Flugzeug eingebaute System nicht benutzbar wäre, da es eine Kollision verhindern würde, könnte ein Terrorist sein eigenes GPS-System mitbringen, welches heute in PDA[121]-Größe erhältlich ist. Die Frage ist auch, ob die Angestellten eines Kraftwerkes die Nebelwerfer auslösen und dann noch schnell genug die verbunkerte Kontrollzentrale erreichen können, um eine Notabschaltung auszulösen, die auf jeden Fall benötigt wird, falls der Angreifer „zufällig“ den Reaktorblock treffen würde.[122]

---

116 Mit Daten sind neben der Sprachübermittlung auch Computerdateien und ähnliches gemeint. Entsprechende Systeme werden jedoch zur Zeit erprobt und sollen möglichst bald Einsatzreife erreichen.

117 Sigrist, Annamaria (2004): *Kampf gegen den Terrorismus: WieDeutschland sich schützen will*, Deutschlandfunk vom 26. Mai 2004, http://www.dradio.de/dlf/sendungen/hintergrundpolitik/268229/ (07.07.2005).

118 Siehe http://www.zdf.de/ZDFde/inhalt/20/0,1872,2213108,FF.html (07.07.2005).

119 An der Umfrage beteiligten sich 1104 Abstimmende, natürlich ist eine solche Umfrage aber nicht repräsentativ.

120 Siehe bspw. die Pläne der EnBW, beschrieben in den Stuttgarter Nachrichten vom 06. Februar .2004 unter dem Titel „Nebelgranaten sollen Atomkatastrophe verhindern“, im Internet zu finden unter: http://www.i-st.net/~buendnis/presse04/msg00021.html

121 PDA = Personal Digital Assistent. Ein kleiner Taschencomputer, welcher ursprünglich dafür gedacht wurde, Termine und Adressen von einem großen Rechner zu übernehmen und auf Reisen bereit zu stellen. Heute sind die Rechner sehr Leistungsstark und eignen sich zur Wiedergabe von multimedialen Inhalten oder eben als Element eines Navigationssystems. Üblicherweise passen die Kleinstrechner in eine Hemdtasche.

122 Hacker, Christina (2004): *Nebel um Isar 1*, in: Umweltnachrichten, Nr. 99, April 2004, http://www.umweltinstitut.org/frames/all/m384.htm (07.07.2005). Der SPD-Bundestagsabgeordnete Berg hält die Vernebelungstaktik für eine sinnlose Billiglösung: „Die Vernebelungstaktik kommt aus dem militärischen Bereich. Während der Angreifer auf ein anderes Ziel abgelenkt wird, können sich die angegriffenen Einheiten

Die zweite Variante basiert auf einer Idee von Professor Eibl, der lange für die Reaktorsicherheitskommission der Bundesregierung gearbeitet hat. Er schlägt vor, Beton-Gitterwände in die möglichen Einflugschneisen der Atomkraftwerke zu bauen. Diese Gitterwände sollten zwischen 15 und 20 Meter groß sein, drei bis fünf Meter dick und 50 Meter entfernt vom Reaktor aufgestellt werden. Die Höhe würde ausreichen (ein Reaktor ist ca. 45 Meter hoch), da die Flugzeuge eine bestimmte Flugbahn wählen müssten. Außerdem würden die Gitter dem Aufprall einer voll beladenen Boeing 747 stand halten. Kleinere Kampfflugzeuge könnten der Mauer zwar ausweichen, wären aber für die Kraftwerke keine Bedrohung. Der Schutz von oben ist, nach Meinung Eibls, nicht so problematisch, da ein Verkehrsflugzeug nicht einfach auf ein Kraftwerk fallen gelassen werden könnte. Weit vor dem Aufprall würde es, aufgrund der entstehenden Kräfte, zerrissen werden. Ein Stahlnetz über dem Reaktor würde vor Hubschraubern schützen, die auf den Reaktor gestürzt werden könnten. Greenpeace hält den Vorschlag für praktikabler als die Einneblungsidee.

Die genannten Beispiele machen deutlich, dass zwar eine offene Diskussion über die Verhinderung von Terroranschlägen geführt wird, dass aber eine Diskussion über die Reaktion auf Terroranschläge ein Nischendasein führt. So wurde dann auch in der „Zeit“ geschrieben, dass die Politik kein Interesse habe, die Bevölkerung über Gefahren aufzuklären, um keine Panik auszulösen. Gleichzeitig sei man aber nach der Abschaffung der Schutzkonzepte aus dem Kalten Krieg nicht mehr genügend vorbereitet (siehe den Abschnitt zu Warnsystemen). So würden wegen Rationalisierungsmaßnahmen sowohl Krankenhausbetten[123] fehlen, als auch die angemessene Ausstattung mit genügend Medikamenten. Ferner diskutieren Politiker eher darüber, ob Krankenwagen mit zwei oder vier Tragen ausstatteten sollte, die Anschaffung jedoch bisher ausblieb.[124]

Neben den Diskussionen zur Prävention und Nachsorge bei Anschlägen ist auffällig, dass es Bedrohungsanalysen entweder nicht gibt oder dass sie äußerst diffus und abstrakt gehalten sind. So wird von Tophoven[125] geschrieben, dass zur Zeit keine Bedrohung durch Terroristen festzustellen ist, dass dieses sich aber ändern könne, quasi über Nacht. Ein Wandel wird damit begründet, dass Deutschland Mitglied in der Anti-Terror Allianz sei und dass es darüber hinaus einige Prozesse gegen des Terrorismus Verdächtigte gibt. Beide Punkte machten Deutschland zu einem nächsten Ziel für Terroranschläge. Außerdem wird darauf hingewiesen, dass es aufgrund ihres angepassten Lebensstils[126] äußerst schwierig sei, mutmaßliche Terroristen zu entdecken. Ähnlich argumentierte der Präsident des Bundesamtes für Verfassungsschutz vor dem ersten Jahrestag des 11. September in der Tageszeitung „die Welt“:[127]

> „Denn unabhängig vom Jahrestag gibt es weltweit, also auch für Deutschland, eine hohe abstrakte Gefahr [...] Wir stehen sicherlich nicht an erster Stelle des Zielspektrums, aber wir sind Feinde. Es wäre sicher in der moslemischen Welt

zurückziehen. Bei einem Angriff auf ein Atomkraftwerk lässt sich ein Terrorist aber weder auf ein anderes Ziel lenken, noch kann ein Reaktor fliehen.“ (Berg, Axel (2004): *Nebelkerzen sind trügerisch*, http://www.axel-berg.de/archiv/pm/040621_terror_akws.pdf (07.07.2005))

123 Nach dem Ende des Kalten Krieges wurden die so genannten zivilen Hilfskrankenhäuser (eine Erklärung zum Phänomen der Hilfskrankenhäuser findet sich auf: http://www.lostplaces.de/hilfskrankenhaus/) abgeschafft und die Hilfszugvereinbarung mit dem Deutschen Roten Kreuz beendet. Nun soll die Bundeswehr in Notfällen mit 30.000 Betten aushelfen. Dies ergibt aber neue Probleme. So würde bei den entsprechenden Einheiten oft auf Reservisten zurückgegriffen, die bei Einsätzen erst vom Arbeitgeber frei gestellt werden müssen. Bei Großereignissen ist dieses aber nicht im Vorhinein zu erwarten. Darüber hinaus ist zu beachten, dass die Bundeswehr auch nur unter bestimmten Bedingungen aushelfen dürfe (Terroranschläge wie die vom 11. September 2001 in den USA würden allerdings unter diese speziellen Bedingungen fallen (Glass, Winfried (2004): *Lazarette ersetzen Zivile Hilfskrankenhäuser*, in: Notfallvorsorge 2004(1), S. 5).

124 Staud, Torafl (2004): *Bloß keine Panik*, in: Die Zeit 2004(19), http://www.zeit.de/2004/19/Zivilschutz (07.07.2005).

125 Tophoven, Rolf (2004): *Ist auch Deutschland vom Terror bedroht?*, in: Notfallvorsorge 2004(2), S. 17-19.

126 Ebd.

127 *Wir stehen nicht im Zielspektrum, sind aber Feinde*, Die Welt, 10. September 2002, http://www.welt.de/data/2002/09/10/444194.html (07.07.2005).

schwerer, einen Angriff auf deutsche Interessen zu vermitteln als auf amerikanische oder auf jüdische."

Weiterführende Forschungsfragen

- Warum findet die öffentliche Diskussion praktisch nur in Bezug auf die Prävention statt und nicht auch im Bereich der Nachsorge bei Terroranschlägen?
- Wie kann die Balance zwischen Sicherheit und Freiheit gewahrt bleiben?
- Müssen „deutsche" Gegebenheiten, die aus der historischen Erfahrung zu erklären sind, wirklich geändert werden (Trennungsgebot, Einsatz der Bundeswehr)?

4. Reaktionen auf Ebene der EU

Obwohl sich diese Studie primär auf Deutschland bezieht, gilt es auch die EU-Ebene zu betrachten, da sowohl Souveränität an die EU abgegeben wurde, als auch bestimmte Funktionen von ihr unter Umständen besser wahrgenommen werden können. Daraus ergeben sich auch Konsequenzen für die Prävention von Terroranschlägen und die Reaktion auf Anschläge. Dabei ist auf europäischer Ebene zwischen mindestens zwei unterschiedlichen Sichtweisen zu unterschieden. Auf der einen Seite versucht die Gemeinschaft, die Anstrengungen und Ressourcen der einzelnen Mitgliedstaaten zu bündeln und als vernetzende Instanz zu wirken. Auf der anderen Seite wird Forschung im Bereich Sicherheit unterstützt, die auch auf die Verhinderung von Anschlägen und die Verminderung des Schadens abzielt.

A) Informationsvernetzung

Die Vorbereitung auf Terroranschläge begann auf europäischer Ebene nach den Anschlägen des 11. September 2001 und wurde noch einmal nach den Anschlägen des 11. März 2004 verstärkt. Der Europäische Rat beauftragte 2001 den Rat und die Kommission einen Plan zur Verbesserung der Kooperation bei biologischen und chemischen Terroranschlägen zu entwerfen. Ende 2002 wurde dann von der Kommission und dem Rat das „Programme To Improve Cooperation In The European Union For Preventing And Limiting The Consequences Of Chemical, Biological, Radiological Or Nuclear Terrorist Threats"[128] (CBRN-Programme) verabschiedet. Das Programm konzentriert sich auf die Bedrohung durch Terroranschläge im CBRN-Bereich und listete sieben strategische Ziele von der Verbesserung der Risikoanalyse bis hin zu einer effizienten Nutzung und Koordination der durch das Programm implementierten Instrumente auf. Das Hauptmerkmal der Ziele ist das Sammeln und Verteilen von Informationen. Das erweiterte Programm von 2004 (revised / widened CBRN Programme)[129] beschränkt sich nicht nur auf den CBRN-Terrorismus, sondern umfasst alle Formen des Terrorismus und legt darüber hinaus einen Schwerpunkt auf den Schutz Kritischer Infrastrukturen und anderen so genannten „soft targets" wie Menschenansammlungen oder die Nahrungskette. Dadurch ist es zu einer deutlichen thematischen Ausweitung der Anstrengungen gekommen. Auch bei dem erweiterten Programm sieht die EU ihre Hauptaufgabe im Sammeln von Informationen und der Vernetzung der einzelnen Mitgliedsstaaten. Dabei wird im Programm hervorgehoben, dass

[128] Siehe http://forum.europa.eu.int/Public/irc/sanco/bichahsbio/library?l=/programme_cooperation/programme_14627f2/_EN_1.0_&a=d (07.07.2005)
[129] http://ue.eu.int/uedocs/cmsUpload/15480EU_Solidarity_Programme.pdf (07.07.2005)

das Subsidiaritätsprinzip zu beachten sei und deshalb eine Beschränkung auf grenzüberschreitende Strukturen und Bedrohungen zu erfolgen habe.

Speziell zugeschnitten auf die Prävention und die Nachsorge bei Terroranschlägen sind die Dokumente KOM(2004) 698[130], 701[131] und 702[132] der Kommission vom 20. Oktober 2004 und in Teilen der Europäische Plan zur Bekämpfung des Terrorismus.[133] Die Nachsorgen bei Großkatastrophen (Terroranschläge haben letztendlich ähnliche Auswirkungen wie Naturkatastrophen) auf Ebene der Union erfolgt über das Beobachtungs- und Informationszentrum (Monitoring and Information Center - MIC). Der betroffene Staat kann das MIC um Hilfe ersuchen. Von dort wird bei den anderen Mitgliedsstaaten angefragt, welche Hilfen sie bieten könnten. Aus diesem Katalog kann der betroffene Staat dann wieder Hilfeleistungen auswählen. Das MIC ist im Direktorat D (Life Program, Legal Implementation and Civil Protection) innerhalb des Environment DG (Directorate General)[134] angesiedelt. Die Personaldecke des MCI ist sehr dünn. Im Juni 2004 arbeiteten dort 14-15 Mitarbeiter. Schließt man die administrativen Beschäftigten ein, sind es ca. 20 Mitarbeiter. Allerdings ist hervorzuheben, dass sich die Mitarbeiterzahl seit 2002 mehr als verdoppelt hat.[135] Darüber hinaus besteht ein Schulungsprogramm, welches Experten der einzelne Staaten auf der einen Seite unterrichtet, auf der anderen Seite aber auch ein Gesprächsforum bilden soll, um die Kommunikation zwischen den Staaten zu verbessern. Daneben vernetzt und sammelt die Kommission das Wissen der EU-Mitglieder in Bezug auf Schwachstellen, Fähigkeiten und Ressourcen im Bereich des Zivilschutzes. In die Bemühungen eingebunden werden auch die nationalstaatlichen Streitkräfte in einer Datenbank über deren Fähigkeiten bei der Reaktion auf Terroranschläge.

Bei der Kommission selbst laufen unterschiedliche Netzwerke zusammen, die zur Gefahrenerkennung, -abwehr und -bewältigung dienen können. Es handelt sich um folgende Informationsaustauschbereiche:

- radiologische Notfälle (ECURIE, European Community Urgent Radiological Information Exchange)[136],
- biologische und chemische Anschlägen (BICHAT, Biological and Chemical Attacks and Threats)[137],
- Non-Food Produkte zum Schutz/ zur Sicherheit des Verbrauchers (RAPEX, The Rapid Alert System for Non-Food Products)[138],
- Schutz des Verbrauchers vor Lebensmittelvergiftungen etc. (RASSF, Rapid Alert System for Food and Feed)[139],
- übertragbare Krankheiten (EWRS, Early Warning and Response System on Communicable Diseases)[140],

130 Kommission der Europäischen Gemeinschaften (2004): *Mitteilung der Europäischen Kommission an den Rat und das Europäische Parlament. Terroranschläge – Prävention, Vorsorge und Risiken,* KOM(2004) 698 – endgültig, Brüssel, http://europa.eu.int/comm/councils/bx20041216/com_2004_698_de.pdf (07.07.2005)

131 Kommission der Europäischen Gemeinschaften (2004): *Mitteilung der Europäischen Kommission an den Rat und das Europäische Parlament. Abwehrbereitschaft und Folgenbewältigung bei der Terrorismusbekämpfung,* KOM(2004) 701 – endgültig, Brüssel, http://europa.eu.int/comm/councils/bx20041216/com_2004_701_de.pdf (07.07.2005)

132 Kommission der Europäischen Gemeinschaften (2004): *Mitteilung der Europäischen Kommission an den Rat und das Europäische Parlament. Schutz kritischer Infrastrukturen im Rahmen der Terrorismusbekämpfung* KOM(2004) 702 – endgültig, Brüssel, europa.eu.int/comm/justice_home/doc_centre/ criminal/terrorism/doc/com_2004_702_de.pdf (07.07.2005).

133 *EU Plan of Action on Combating Terrorism – Update*, http://ue.eu.int/uedocs/cmsUpload/EUplan16090.pdf (07.07.2005).

134 Siehe http://europa.eu.int/comm/environment/index_de.htm (07.07.2005).

135 Lindstrom, Gustav (2004): *Protecting the European homeland – the CBR Dimension*, Chaillot Paper Nr. 69, S. 50.

136 Siehe http://rem.jrc.cec.eu.int/ecurie/ (07.07.2005).

137 Siehe http://europa.eu.int/scadplus/leg/de/cha/c11576.htm (07.07.2005).

138 Siehe http://europa.eu.int/comm/dgs/health_consumer/dyna/rapex/rapex_en.cfm (07.07.2005).

139 Siehe http://europa.eu.int/comm/food/food/rapidalert/index_en.htm (07.07.2005).

140 Siehe http://europa.eu.int/comm/health/ph_threats/com/early_warning_en.htm (07.07.2005).

- Gesundheitskontrollen bei tierärztlich relevanten Einfuhren (SHIFT)[141] und
- Tiergesundheit (ADNS, Animal Desease Notification System).[142]

Die Bereiche sind zurzeit noch nicht untereinander vernetzt, auch wenn alle bei der Europäischen Kommission zusammen laufen. Es wird darüber nachgedacht, ob eine solche übergeordnete Vernetzung unter dem Namen ARGUS erfolgen soll.

Der Schutz Kritischer Infrastrukturen ist auf Europäischer Ebene noch nicht so deutlich etabliert, wie traditionelle Gefahren durch radiologische, atomare, biologische und chemische Stoffe oder (Tier-)Seuchen. In Zukunft soll aber offensichtlich ein größeres Augenmerk auf den Schutz dieser Strukturen gerade vor Terroranschlägen, gelegt werden.[143] In diesem Zusammenhang ist die Schaffung eines Frühwarnsystems (EPCIP) nach dem Vorbild der schon bestehenden Netze zu nennen. Dabei soll das EPCIP den Informationsaustausch über gemeinsame Gefährdungen und Bedrohungen erleichtern. Außerdem will die Kommission sektorspezifische Sicherheitsstandards und Normen vorschlagen, in denen es noch keinen solchen Bemühungen gibt. Das Ziel der Bemühungen soll es sein, einen einheitlichen Sicherheitsstandard in Bezug auf die Kritischen Infrastrukturen in der gesamten Europäischen Union zu erreichen. Darüber hinaus soll es so wenig Angriffspunkte wie möglich geben und die öffentliche Ordnung soll nach einem Angriff zügig wieder hergestellt werden können.

Neben den Bemühungen der Kommission ist der „EU Plan of Action on Combating Terrorism“ zu nennen und in diesem besonders das Ziel fünf „To enhance the capability of the European Union and of its Member States to deal with the consequences of a terrorist attack“. Der Plan stellt eine Art „Road Map“ zur Bekämpfung des Terrorismus und seiner Folgen dar und geht über die Verminderung von Schäden hinaus, indem er Ziele wie Grenzsicherheit definiert oder Schritte zur Vermeidung von Terrorismus beschreibt.

Viele Ansätze im Bereich Informationen beinhalten die Vernetzung von Wissen und bauen auf den Mitarbeitswillen der beteiligten Staaten. Werden keine Informationen oder Ressourcen zur Verfügung gestellt, funktionieren die Netzwerke nicht. Genauso basiert das System darauf, dass die gesammelten Informationen abgerufen werden. Geschieht das nicht, sind die Netzwerke wertlos. Genauso hat es sich bspw. bei den Waldbränden 2003 in Portugal gezeigt. Die politische Bereitschaft zu helfen wurde von 21 Staaten signalisiert. Nur drei Staaten schickten dann aber Hilfe.[144]

B) Forschungsprogramme

Der zweite Ansatzpunkt in der Vorbereitung gegen Terroranschläge erfolgt im Bereich der Forschung. Hier unterstützt die EU wissenschaftliche Einrichtungen und die Industrie, um eine Erhöhung der Sicherheit der Bürger zu erreichen und gleichzeitig die Wettbewerbsfähigkeit der europäischen Industrie zu verbessern. Zentrale Anlaufstelle für Informationen um das Unterstützungsprogramm ist eine Webseite.[145] Zurzeit laufen noch so genannte vorbereitende Maßnahmen (Preparatory Action on Security Research, PASR) (von 2004-2006), die folgende Prioritäten haben:[146]

---

141 Siehe http://europa.eu.int/scadplus/leg/de/lvb/l11036.htm (07.07.2005).
142 Siehe http://europa.eu.int/comm/food/animal/diseases/adns/index_en.htm (07.07.2005). Siehe auch KOM(2004) 701.
143 KOM(2004) 702.
144 Lindstrom, Protecting the European homeland, S. 50.
145 Siehe http://europa.eu.int/comm/enterprise/security/index_en.htm (07.07.2005).
146 De Smet, Pieter (2004): *Towards a European Security Research Programme (ESRP)*, Präsentation gehalten auf der Konferenz „Sicherheitsforschung in der Europäischen Union“ am 14. Dezember 2004 in Mühlheim an der Ruhr, veranstaltet von ZENIT, S. 13, 17.

- Verbesserung des Situationsbewusstseins,
- Optimierung der Sicherheit und des Schutzes vernetzter Systeme,
- Schutz vor Terrorismus,
- Verbesserung des Krisenmanagements und
- die Interoperabilität und Integration von Systemen zur Information und Kommunikation.

2004 wurden elf Anträge angenommen, welche die fünf genannten Bereiche umfassen. Diese beinhalten unter anderem die Entwicklung von Detektoren zum Aufspüren von gefährlichen Stoffen (TERASEC), die Ausarbeitung von Krisenmanagement Systemen (CRIMSON, ISCAPS), Forschung zum Schutz kritischer Infrastrukturen (VITA) und andere.[147]

Bei dem Forschungsprogramm wird das Hauptaugenmerk auf die Prävention gelegt und weniger auf eine Reaktion nach einem Terroranschlag. Die Bemühungen, die „Sicherheitsforschung" innerhalb der Europäischen Union voran zu treiben, werden alleine schon durch das dafür aufgewandte Budget deutlich. So schlägt die „Group of Personalities in the field of Security Research" in ihrem Bericht[148] vor, dass zusätzlich zu den aktuellen Mitteln ab 2007 eine Summe von einer Milliarde Euro aufgewendet werden solle. Allerdings scheint sich die Kommission eher auf technische und industriell gestützte Problemlösungen zu verlassen, als auch andere Bereiche mit einzubeziehen.

Neben den Programmen der Kommission und des Rates ist im Zusammenhang mit der Prävention von Terrorismus die „Erklärung zur Solidarität gegen Terrorismus"[149] zu nennen, welche kurz nach den Terroranschlägen vom Madrid 2004 verabschiedet wurde. In der Erklärung wird die Solidarität der Mitgliedsstaaten untereinander im Falle eines Anschlages festgeschrieben. Als Reaktion auf und als Prävention vor Terroranschläge können alle Mittel der Staaten mobilisiert werden, unter anderem auch militärische.

Weiterführende Forschungsfragen

- Werden die Informationsnetze der Kommission durch die Staaten genutzt?
- Wie funktioniert das Katastrophenmanagement innerhalb der EU?
- Welche Erfolge sind durch die Forschungsprogramme erreicht worden oder könnten erreicht werden?

5. Zusammenfassung

Die Anschläge vom 11. September 2001 in New York und Washington und der Anschlag vom 11. März 2004 in Madrid haben deutlich gemacht, dass sich die Staaten auf eine neue Formen des internationalen Terrorismus einstellen müssen, dem es darum geht, möglichst viele Menschen zu töten. Die Risikobereiche Nuklearterrorismus und Kritische Infrastrukturen zeigen die Ambivalenz der aktuellen Situation. Die Sicherheit von Anlagen und Lagern, die nukleare, biologische und chemische Substanzen enthalten sollte zentral sein. Andererseits hätten Anschläge mit Hilfe von verstrahltem Material keine tödliche Auswirkung auf viele Bürger eines Landes. Ein Anschlag mit so einer Waffe würde allerdings zu einer Lähmung großer Areale führen. Genauso ist bei einem Anschlag auf Kritische

[147] Vgl. European Commission (2004): *Results of the First Call – List of funded Activities*, http://europa.eu.int/comm/enterprise/security/articles/article_2164_en.htm (07.07.2005).
[148] Group of Personalities in the field of Security Research (2004): *Research for a Secure Europe. Report of the Group of Personalities in the Field of Security Research*, http://europa.eu.int/comm/research/security/pdf/gop_en.pdf (07.07.2005).
[149] Europäische Union (2004): *Erklärung zur Solidarität gegen den Terrorismus*, http://europa.eu.int/abc/doc/off/bull/de/200403/i1050.htm (07.07.2005).

Infrastrukturen mit weiträumigen Störungen und im schlimmstem Fall mit einem partiellen Ausfall von Wirtschaftszweigen zu rechnen. Terroranschläge mit den genannten Methoden sind deshalb nicht als Anschläge mit Massenvernichtungswaffen zu bezeichnen, sondern als Anschläge mit „Weapons of Mass Disruption“. Anschläge in den genannten Bereichen sind bisher noch nicht erfolgt. Einerseits könnte man daraus die Vermutung ableiten, dass Terrororganisationen nicht fähig sind, die Verwundbarkeit in den genannten Bereichen auszunutzen. Andererseits sollte angestrebt werden, die Strukturen so gut es geht zu schützen, da eine Risikoreduktion sicherlich besser ist als darauf zu vertrauen, dass terroristische Organisationen entsprechende Fähigkeiten nicht entwickeln werden. Die Verbesserung nuklearer Sicherheit von Produktionsanlagen, Lagern und Forschungsstätten muss zudem zentrale Aufgabe staatlicher Anstrengungen sein und forciert werden.

In Deutschland wurden nach dem Zusammenbruch des Warschauer Pakts Zivilschutzfähigkeiten abgebaut, da der Verteidigungsfall von da an als äußerst unwahrscheinlich galt. Die Strukturen des Zivilschutzes sind zum Teil nicht nur im Verteidigungsfall nützlich, sondern auch bei anderen Katastrophen wie Überschwemmungen oder Großunfällen. Diese Erkenntnis ist im Lauf der letzten Jahre wieder in das Bewusstsein der Fach- und Regierungskreise gelangt, wodurch eine allmähliche Verbesserung des Bevölkerungs- und Katastrophenschutzes zu erwarten ist, insbesondere auch auf europäischer Ebene. Gleichzeitig beschränken sich administrative Maßnahmen hauptsächlich auf die Prävention von und weniger auf die Vorsorge für die Folgen eventueller Terroranschlägen.

In der wissenschaftlichen und gesellschaftlichen Diskussion wird deutlich, dass von einigen Politikern und Autoren eine Aufweichung der Erfahrungen der Vergangenheit gefordert wird, sei es beim Einsatz des Militärs für Zwecke der „inneren Sicherheit“ oder bei der Trennung von Geheimdiensten und Polizei. In ähnlicher Weise wird eine höherer Grad an Zentralisierung gefordert. Neben der Nennung möglicher „Hindernisse“ bei der Strafverfolgung und beim Schutz von Objekten ist auffällig, dass es keine Erkenntnisse über mögliche Bedrohungen gibt. So wird argumentiert, dass es zur Zeit eine abstrakte Bedrohung gäbe, die sich aber jederzeit in eine reale ändern könnte. Verbindet man beide Aspekte, ist auffällig, dass eine Ausweitung der Rechte von Strafverfolgungsbehörden gefordert wird, diese Ausweitung aber nur unzureichend begründet und mit sehr vielen Konjunktiven verbunden ist.

Auf Ebene der EU sind Bemühungen zur Bekämpfung von Terrorismus und zur Katastrophenabwehr und -bewältigung deutlich zu erkennen. Dabei ist besonders der Ansatz hervorhebenswert, Ressourcen gemeinsam zu nutzen und Anstrengungen auf EU-Ebene zu koordinieren. In Zeiten leerer Kassen ist eine Teilung von Gerät, Wissen und Personal sicherlich ein sehr sinnvoller Ansatz, gerade weil nicht zu erwarten ist, dass sich an vielen Orten gleichzeitig eine Katastrophe ereignen wird. Allerdings gilt es wiederum zu beachten, dass die EU sehr wenig eigene Kompetenzen hat und auf die Kooperation der Mitgliedsstaaten angewiesen ist. Im Bereich der Forschung scheint eher die technisch-industrielle Aufgabenstellungen zu überwiegen, womit auf der einen Seite den USA nachgeeifert wird und auf der anderen Seite aktive Wirtschaftshilfe für die eigene industrielle Basis zu betreiben. Hier wäre es sicherlich besser, größeres Augenmerk auf gesellschaftliche Problemlösungen und ethische Überlegungen zu richten. Zur Zeit entsteht das Gefühl, dass das EU Sicherheitsforschungsprogramm eher eine versteckte Industrie- und Rüstungssubvention ist, denn ein umfassendes Programm zur Verbesserung der europäischen Sicherheit.

Die Frage, ob Deutschland auf Terroranschläge vorbereitet ist, lässt sich natürlich nicht eindeutig beantworten. Einerseits ist der Katastrophenschutz in Deutschland sicherlich einer der am besten ausgestatteten der Welt, gerade was die Anzahl der Helfer ausmacht. Auf der anderen Seite gibt es offensichtlich für mache Situationen, wie eine Epidemie oder ein großflächiger Angriff mit radioaktivem Material, keine oder nur unzureichende

Vorbereitungen. Hier sind vor allem die Sparanstrengungen gerade im Gesundheitsbereich eine Ursache für zu geringe Anstrengungen identifizieren. Des weiteren ist auffällig, dass in der Diskussion eher für mehr Sicherheit plädiert wird, gerade auf Kosten der individuellen Freiheit. Die Bedrohung hingegen scheint in den Hintergrund zu treten. Gerechtfertigt werden die Begehrlichkeiten damit, dass sich die „abstrakte“ Bedrohungslage jederzeit ändern könne und man deswegen vorbereitet sein müsse.

Die vorliegende Forschungsstudie kann, aufgrund der beschränkten Bearbeitungszeit, nur einen kursorischen Überblick über die Verwundbarkeit Deutschlands und den Stand der Vorbereitung auf eventuelle Großunfälle liefern. Aus ihr lassen sich allerdings einige Forschungsfragen ableiten, welche im Rahmen eines Workshops beantwortet werden soll. Die Frage nach der Verwundbarkeit industrieller Ziele (Raffinerien, Energieerzeugung etc.) bedarf dabei genauso sorgfältiger Durchdringung wie die Frage nach der maritimen Sicherheit und der Anfälligkeit von Transportnetzwerken und Knotenpunkten (Häfen, Flughäfen, Verkehrsknoten etc.). Beispielsweise stellt sich generell die Frage, wie Deutschland beim Einsatz von „Weapons of Mass Disruption“ reagieren kann. Eine völliger Schutz vor dieser Art von Ereignissen ist nicht möglich. Dennoch kann versucht werden, die Auswirkungen lokal und zeitlich begrenzt zu halten, wodurch eine schnelle Rückkehr zum Normalzustand zu erreichen wäre. Genau so stellt sich die Frage, welche Maßnahmen zu einem besseren und schnellerem Katastrophenmanagement führen könnten. Auf Ebene der EU sollte versucht werden, eine bessere Kooperation zwischen den einzelnen Staaten verbindlich fest zu schreiben. Nur wie ist eine solche Festschreibung möglich und welche Schritte müssen dafür unternommen werden? Zu dem abzuhaltenden Workshop sollten ca. zehn Experten eingeladen werden, die vorher ein Papier zu einer vorgegebenen Fragestellung aus ihrem Gebiet erstellt haben. Einige Fragestellungen wurden in der vorliegenden Studie identifiziert. Darüber hinaus ist es wünschenswert, dass ein solcher Workshop möglichst noch vor der Sommerpause abgehalten wird, um weiterführende Forschungsarbeiten im Bereich der für diese Forschungsstudie relevanten Fragestellung zu ermöglichen.

6. Weiterführende Literatur

A) Staatliche Dokumente

Bundesministerium des Innern (2004): *Nach dem 11. September 2001: Maßnahmen gegen den Terror*, Dokumentation aus dem Bundesministerium des Innern.

Bundesverwaltungsamt, Zentralstelle für Zivilschutz (2003): *Neue Strategie zum Schutz der Bevölkerung in Deutschland*, Gebrr. Klingenberg Buchkunst Leipzig GmbH

GAO (2003): *Critical Infrastructure Protection - Challenges in Securing Control Systems*, GAO-04-140T, http://www.gao.gov/cgi-bin/getrpt?GAO-04-140T (08.06.2004)

National Commission on Terrorism (2001): *Countering the Changing Threat of International Terrorism, Report of the National Commission on Terrorism*, Washington D.C.

Reaktorsicherheitskommission (2001): *Sicherheit deutscher Atomkraftwerke gegen gezielten Absturz von Großflugzeugen mit vollem Tankinhalt*, http://www.bmu.de/files/stellungnahme_rsk.pdf (07.07.2005)

Schutzkommission beim Bundesministerium des Inneren (2001): *Zweiter Gefahrenbericht*, Schriftenreihe der Schutzkommission beim Bundesministerium des Inneren Nr. 48

Ständige Konferenz der Innenminister und -senatoren der Länder (2002): *Neue Strategie zum Schutz der Bevölkerung in Deutschland*, http://www.thw-hannover.de/inh/tipstren/trends/IMK.html (07.07.2005)

B) Zeitungsartikel

Brost, M. / Uchatius, W. (2001): *Die Entdeckung der Verwundbarkeit*, in: Die Zeit 2001(40), S.19-20

Drösser, Christopher / Krempl, Stefan (2000): *Das Schlachtfeld der Zukunft ist der Cyberspace*, in: Die ZEIT 2/2000

Rauner, Max / Schuh, Hans (2004): *Stunde der Nebelwerfer*, in: Die Zeit 11/2004, http://www.zeit.de/2004/11/Atomterror1 (07.07.2005)

Stoldt, Till-R. (2004) Ein Gitter fängt die Maschinen ab, in: Welt am Sonntag, 18.07.2004, http://www.wams.de/data/2004/07/18/306974.html (07.07.2005)

Randow, G. von (2002): *So baut man eine Panik-Bombe*, in: Frankfurter Allgemeine Sonntagszeitung, 16. März 2002, Nr. 24, S.76

C) Monografien und Aufsätze

Ackerman, Gary A. / Bale, Jeffrey M. (2002): *Al-Qa`ida and Weapons of Mass Destruction*, http://cns.miis.edu/pubs/other/alqwmd.htm (07.07.2005).

Albright, David (2002): *Al Qaeda's Nuclear Program: Through the Window of Seized Documents*, Special Forum 47, Berkeley, Cal.: Nautilus Institute

Albright, David /O'Neill, Kevin /Hinderstein, Corey (2001): *Nuclear Terrorism: The Unthinkable Nightmare*, ISIS Issue Brief, 13. September 2001

Antes, Manfred (2002): *Sicherheitspolitische Herausforderungen moderner Informationstechnologie*, http://www.auswaertiges-amt.de/www/de/infoservice/download/pdf/friedenspolitik/cyberwar.pdf (03.06.2004)

Berkowitz, Bruce (2000): *Information Warfare: Time to Prepare*, in: Issues in Science and Technology Online, Winter 2000, http://www.issues.org/issues/17.2/berkowitz.htm (12.11.2003)

Borchgrave, Arnaud de et al (2000): *Cyber Threats and Information Security Meeting the 21st Century Challenge*, Center for Strategic and International Studies, Washington D.C.

Bos, Ellen (Hrsg.) (2003): *Neue Bedrohung Terrorismus: der 11. September 2001 und die Folgen*, Münster

Boutwell, Jeffrey / Calogero, Francesco /Harris, Jack (2002): *Nuclear Terrorism: The Danger of Highly Enriched Uranium*, Pugwash Issue Brief Jg. 2, Nr. 1, http://www.pugwash.org/publication/pb/pblist.htm (07.07.2005)

Brown, Alan S. (2002): *SCADA vs. The hackers,* in: mechanical engineering, http://www.memagazine.org/backissues/dec02/features/scadavs/scadavs.html (10.05.2004)

Bunn, Matthew (2000): *The Next Wave: Urgently needed new steps to arms control warheads and fissile materials*, http://ksgnotes1harvard.edu/BCSIA/Library.nsf/pub/Nextwave (08.06.2004)

Bunn, Matthew / Anthony Wier (2004): *Securing the Bomb. An Agenda for Action*, Cambridge/Mass.: Project on Managing the Atom, Belfer Center for Science and International Affairs, Harvard University

Bunn, Matthew / Holdren, John / Wier, Anthony (2002): *Securing Nuclear Warheads and Materials: Seven Steps for Immediate Action*, www.nti.org/e_research/securing_ nuclear_weapons_and_materials_May2002.pdf (07.07.2005)

Calogero, Francesco (2001): *Nuclear Terrorism, Speech given at the Nobel Prize Symposium „The Conflicts of the 20th century and the Solutions for the 21st Century"*, 6. bis 8. Dezember2001, http://www.pugwash.org/September11/sept11-calogero.htm (07.07.2005)

Cameron, Gavin (2000): *WMD Terrorism in the United States: The Threat and Possible Countermeasures*, in: The Nonproliferation Review, Jg. 7, Nr. 1, S. 162-179

Chyba, Christopher F. / Greninger, Alex L. (2004): *Biotechnology and Bioterrorism: An Unprecedented World*, in: Survival, Jg. 46, Nr. 2, S. 143-162

Clarke, Richard (1998): *America's Fight against Terrorism: At Home and Abroad*, Rede auf der Policy Konferenz im Lansdown Conference Center am 16 Oktober 1998, http://www.washingtoninstitute.org/templateC07.php?CID=78 (23.06.2004)

Collmer, Sabine / Kümmel, Gerhard (Hrsg.) (2003): *Asymmetrische Konflikte und Terrorismusbekämpfung: Prototypen zukünftiger Kriege?*, Nomos

Danwitz, Thomas von (2002): *Rechtsfragen terroristischer Angriffe auf Kernkraftwerke*, Bochumer Beiträge zum Berg- und Energierecht, Nr. 36

Denning, Dorothy E. (2001): *Is Cyber Terror Next?*, in: Social Science Research Council: After September 11, http://www.ssrc.org/sept11/essays/denning.htm (26.04.2004)

Denning, Dorothy E. (2001a): Cyberwarriors - Activists and Terrorists Turn to Cyberspace, in Harvard International Review, Jg. 23, Nr. 2, 70-75, http://hir.harvard.edu/articles/?id=905 (12.11.2003)

Dunn, Myriam / Wigert, Isabelle (2004): *Critical Information Infrastructure Protection*, Center for Security Studies, Zürich

Erbel, Günter (2002): *Die öffentliche Sicherheit im Schatten des Terrorismus*, in: Aus Politik und Zeitgeschichte, B 10-11, S. 17- 21

Falkenrath, R.A. / Newman, R.D./ Thayer, B.A. (1998): *America´s Achilles´ Heel. Nuclear, Biological, and Chemical Terrorism and Covert Attack*, BCSIA Studies in International Security

Forschungsinstitut der Deutschen Gesellschaft für Auswärtige Politik (Hrsg.) (2004): *Homeland security: die Bedrohung durch den Terrorismus als Herausforderung für eine gesamtstaatliche Sicherheitsarchitektur*, Berlin

Frank, Hans / Hirschmann, Kai (Hrsg.) (2002): *Die weltweite Gefahr, Terrorismus als international Herausforderung*, Berliner Verlag

Garwin, R.L. / Charpak, G. (2001): *Megawatts and Megatons - A Turning Point in the Nuclear Age?*, Alfred A. Knopf Publisher.

Geier, Wolfram (2002): *Zivilschutz im Wandel, Herausforderungen, Probleme und Lösungen im 21. Jahrhundert*, in: Bevölkerungsschutz 2002(1), S. 4-9

Goetz, Eric (2002): *Cyber Security of the Electric Power Industry*, Institute for Security Technology Studies At Dartmouth College, Hanover http://www.ists.dartmouth.edu/ISTS/ists_docs/cyber_security_electric.htm (16.02.2004)

Guiwa-Schindler, Analisa (2002): *Die Terroranschläge am 11. September: deutsche Reaktionen auf den internationalen Terrorismus*, utz

Hirsch, Helmut (2001): *Gefährdung deutscher Atomkraftwerke durch den Absturz von Verkehrsflugzeugen*, http://www.greenpeace.org/deutschland/?page=/deutschland/fakten/atom/atomkraftwerke/die-unfriedliche-nutzung-der-atomenergie (07.07.2005)

Holdren, John P. / Bunn, Matthew (2002): T*echnical Background: Controlling Nuclear Warheads and Materials*, http://www.nti.org/e_research/cnwm/overview/technical.asp 07.07.2005)

Hutter, Reinhard (2001): *Risiken im Informationszeitalter*, in: Bundesakademie für Sicherheitspolitik (Hrsg.) (2001): *Sicherheitspolitik in neuen Dimensionen – Kompendium zum erweiterten Sicherheitsbegriff*, Hamburg, S. 483-500

José Martínez Soria (2004): *Polizeiliche Verwendungen der Streitkräfte*, In: Deutsches Verwaltungsblatt 10/2004, S. 597

Knelangen, Wilhelm (2001): *Das Politikfeld innere Sicherheit im Integrationsprozess. Die Entstehung einer europäischen Politik der inneren Sicherheit*, Leske & Budrich

Knies, Gerhard (Hrsg.) (1990): *Betriebsbedingung Frieden: Herausforderungen der Hochtechnologie-Zivilisation für eine nachmilitärische Ära*, Brandenburgisches Verlags-Haus

Kulick, Holger (2001): *Das "Restrisiko" ist plötzlich riesengroß*, in: Der Spiegel Nr. 16,

Lawson, Shannon M. (2002): *Information Warfare: An Analysis of the Threat of Cyberterrorism Towards the US Critical Infrastructure SANS Institute*, http://www.sans.org/rr/papers/29/821.pdf (15.09.03)

Le Guelte, Georges (2003): *Terrorisme Nucléaire. Risque majeur, fantasme ou épouvantail?*, Guelte Georges LE

Lewis, James A. (2002): *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*, Center for Strategic & International Studies, http://www.csis.org/tech/0211_lewis.pdf (31.05.2004)

Lutz, Dieter S. (2001): *Sicherheit trotz Verwundbarkeit?*, http://www.ifsh.de/dokumente/artikel/65_Terror.doc (07.07.2005)

Lutz, Dieter S. (2001): *Terrorismus, Solidarität und Verwundbarkeit. Der 11. September 2001: Ursachen und Folgen aus Sicht der Friedensforschung*, in: Forschung & Lehre 2001(8)

Ma, Chunyan / Hippel, Frank von (2001): *Ending the Production of Highly Enriched Uranium for Naval Reactors*, in: The Nonproliferation Review, Jg. 8, Nr. 1, S. 86-101

Maerli, Morten Bremer (2000): *Relearning the ABCs: Terrorists and Weapons of Mass Destruction*, in: The Nonproliferation Review, Jg. 7, Nr. 2, S. 108-119

McCloud, Kimberly / Osborne, Matthew (2002): *WMD Terrorism and Usama Bin Laden*, CNS-Report, Monterey/cal., http://cns.miis.edu/pubs/reports/binladen.htm (07.07.2005)

Mitsilegas, Valsamis / Monar, Jörg / Rees, Wyn (2003): *The European Union and Internal Security. Guardian of the People?,* Palgrave

Moteff, John D. (2001): *Critical Infrastructures: Background, Policy, and Implementation*, CRS Report to Congress RL 30153, http://fpc.state.gov/documents/organization/7947.pdf (04.06.2004)

Müller, Thorsten (2003): *Integrierte Innen- und Justizpolitik der EU. Eine Analyse der Integrationsentwicklung*, Leske & Budrich

Occhipinti, John (2003): *The Politics of EU Police Co-operation. Toward a European FBI?*, Lynne Rienner

Odenthal, Klaus W. (2003): *Der Schutz Kritischer Infrastrukturen*, in Hirschmann, Kai / Leggemann, Christian (Hrsg.) (2003): *Der Kampf gegen den Terrorismus. Strategien und Handlungserfordernisse in Deutschland*, Berliner Wissenschaftsverlag, S. 281-318

Piper, Gerhard (2002): *Terrorziel USA? Strukturelle Verwundbarkeit als Legitimation des Überwachungsstaates*, http://www.bits.de/public/articles/ami/ami0902.htm (07.07.2005)

Pordesch, Ulrich und Rossnagel, Alexander (1997): *Untersuchungen zur Verletzlichkeit einer vernetzten Gesellschaft*, in: Lang, C. / Werle, R. (Hrsg.) (1997): *Modell Internet? Entwicklungsperspektiven neuer Kommunikationsnetze*, Campus-Verlag, S. 187ff.

Pordesch, Ulrich (1989): *Zum Katastrophenpotential der Telekommunikation*, in: Zivilverteidigung, 1989(11), S. 41ff.

Rinaldi, Steven M. / Peerenboom, James P. / Kelly, Terrence K. (2001): *Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies*, in: IEEE Control Systems Magazine, Dezember 2001, S. 11-25

Ritter, Stefan / Weber, Joachim (2003): *Critical Infrastructure Protection: Survey of world-wide Activities*, Vortrag gehalten auf der Cyber Security and Contingency Planning - Threats and Infrastructure Protection, Universität Zürich-Irchel, Zurich, 25.-27. September, http://www.eda.admin.ch/eda/e/home/foreign/secpe/intsec/wrkshp/pubonl.html (07.07.2005)

Roßnagel, Alexander (1991): *Verletzlichkeit und Komplexität einer informatisierten Gesellschaft*, Arbeitspapiere provet Nr. 69, S. 442 - 446

Roßnagel, Alexander (1995): *Die Verletzlichkeit der Informationsgesellschaft und rechtlicher Gestaltungsbedarf*, in: Kreowski, Hans-Joerg / Risse, Thomas / Spillner, Andreas / Streibl, Ralf und Vossberg, Karin (Hrsg.) (1995): *Realität und Utopien der Informatik*, Agenda Verlag, S. 56 ff.

Roßnagel, Alexander (Hrsg.) (1989): *Die Verletzlichkeit der "Informationsgesellschaft"*, Westdeutscher Verlag

Schmitz, Walter (2003): *Kritische Infrastrukturen: Bedrohungsanalyse und Handlungsbedarf*, Vortrag auf der Konferenz „Netz- und Computersicherheit - Sind wir auf einen Angriff auf unsere Informationssysteme und Informations-Infrastrukturen vorbereitet?“ an der Universität Düsseldorf, http://www.aksis.de/Bedrohung-und-Handlungsbedarf.pdf (03.06.2004)

Schörnig, Niklas (2001): *Demokratischer Frieden durch überlegene Feuerkraft*, HSFK-Standpunkte Nr. 3/2001, http://www.hsfk.de/downloads/sp0301.pdf (07.07.2005)

Schulzki-Haddouti, Christiane (2004): *Im Netz der inneren Sicherheit: die neuen Methoden der Überwachung*, Europa Verlags-Anstalt

Shea, Dana A (2003) *Critical Infrastructure: Control Systems and the Terrorist Threat*, CRS Report for Congress RL31534, http://www.fas.org/irp/crs/RL31534.pdf (04.06.2004)

Smithson, Amy (2000): *Ataxia: The Chemical and Biological Terrorism Threat and the US Response*, Stimson Center Report No. 35, http://www.stimson.org/pub.cfm?id=12 (07.07.2005)

Szukala, Andrea (2004): *Anti-Terror-Politik in Deutschland*, Arbeitspapiere zur Internationalen Politik und Außenpolitik, Lehrstuhl Internationale Politik Universität Köln, http://www.politik.uni-koeln.de/jaeger/downloads/aipa0403.pdf (07.07.2005)

Tammler (2003): *Über den Einsatz der Streitkräfte im Innern zur Abwehr terroristischer Angriffe aus der Luft*, Wissenschaftliche Dienste des Deutschen Bundestages

Theveßen, Elmar (2004): *Bedrohung Deutschlands durch den islamistischen Terrorismus: aktuelle Gefährdungs- und Sicherheitslage in Europa*, in: Möller, Reinhard (Hrsg.) (2004): *Islamismus und terroristische Gewalt*, Ergon-Verlag, S. 153-168

Tucker, Jonathan B. (2004): *Biological Threat Assessment: Is the Cure Worse Than the Disease?*, in: Arms Control Today Oktober 2004,: http://www.armscontrol.org/act/2004_10/Tucker.asp?print (07.07.2005)

Wagner, Wolfgang (2002): *Gegengewicht Demokratisierung Der Europäische Verfassungskonvent und die Politik der inneren Sicherheit in Europa*, HSFK-Standpunkte 2002/6

Weidenfeld, Werner (Hrsg.) (2004): *Herausforderung Terrorismus: die Zukunft der Sicherheit*, Verlag für Sozialwissenschaften

Wenger, Andreas / Metzger, Jan / Dunn, Myriam (2002): *Schutz kritischer Informationsinfrastrukturen - Eine sicherheitspolitische Herausforderung*, in: Europäische Sicherheit, Oktober 2002, http://www.europaeische-sicherheit.de/Rel/ausgaben/10oktober2002/1002,02,01.html (07.07.2005)

Westrin, Peter (2001): *Critical Information Infrastructure Protection (CIIP)*, in: Information & Security Bd. 7, S. 67-79

Wohlleben, Verena (2003): *Zivilschutz – Ein Allgemeiner Überblick*, Entwurf eines Generalberichtes, Parlamentarische Versammlung der NATO, http://www.bundestag.de/parlament/internat/nato_pv/archiv/berichterst/143_CC_03_Wohlleben_-_de.pdf (07.07.2005)

Working Paper von IFAR:

WORKING PAPER #1:
Präventive Rüstungskontrolle

WORKING PAPER #2:
Die Raketenprogramme Chinas, Indiens und Pakistans sowie Nordkoreas – Das Erbe der V-2 in Asien

WORKING PAPER #3:
Weapons of Mass Destruction in the Near and Middle East - After the Iraq War 2003

WORKING PAPER #4:
Streitkräftemodernisierung und ihre Auswirkungen auf militärische Bündnispartner

WORKING PAPER #5:
Der Schutz Kritischer Infrastrukturen

WORKING PAPER #6:
Terrorgefahr und die Verwundbarkeit moderner Industriestaaten: Wie gut ist Deutschland vorbereitet?

Kontakt:
Götz Neuneck
Interdisziplinäre Forschungsgruppe Abrüstung und Rüstungskontrolle IFAR

Institute for Peace Research and Security Policy at the University of Hamburg
Falkenstein 1, 22587 Hamburg
Tel: +49 40 866 077-0 Fax: +49 40 866 36 15
ifar@ifsh.de www.ifsh.de
Webpage zur Rüstungskontrolle: www.armscontrol.de